[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H01L 23/58

[12] 发明专利申请公开说明书

[21] 申请号 00818715.0

[43] 公开日 2003 年 7 月 30 日

[11] 公开号 CN 1433576A

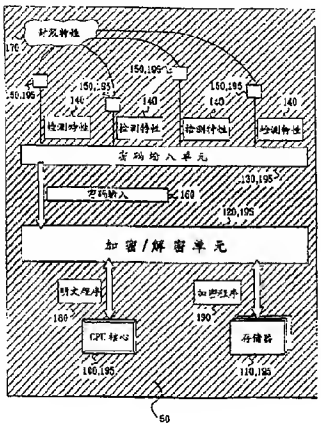
[22] 申请日 2000.12.27 [21] 申请号 00818715.0
[30] 优先权
[32] 1999.12.30 [33] US [31] 60/173,994
[86] 国际申请 PCT/IB00/02021 2000.12.27
[87] 国际公布 WO01/50530 英 2001.7.12
[85] 进入国家阶段日期 2002.7.30
[71] 申请人 奥利弗·克默林
地址 德国里德伯格
共同申请人 弗里策·克默林
[72] 发明人 奥利弗·克默林 弗里策·克默林
[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 李 辉

权利要求书 3 页 说明书 27 页 附图 24 页

[54] 发明名称 集成电路的防窜改封装

[57] 摘要

本发明披露了一种集成电路装置，包括：电路，采用加密过程；以及保护部件(例如：封装层)，可以减少对电路的访问；其中该电路响应保护部件的至少一个物理参数进行加密和/或解密(例如：通过从其读取密钥)，使得通过窜改保护部件来访问电路会使加密过程和/或解密过程发生变化。



ISSN1008-4274

1. 一种集成电路装置，包括：电路，采用加密过程；以及保护部件，用于减少对电路的访问；其特征在于，该电路响应于保护部件的至少一个物理参数进行加密和/或解密，使得通过窜改保护部件来访问电路会改变加密过程和/或解密过程。

2. 根据权利要求 1 所述的装置，其中该电路包括在其内以加密形式存储数据的存储器。

3. 根据权利要求 1 所述的装置，其中该电路包括用于连接一个单独存储装置的总线。

4. 根据权利要求 1 所述的装置，其中保护部件包括围绕该电路的封装。

5. 根据权利要求 1 所述的装置，其中该电路包括加密器，该加密器对数据应用加密和/或解密算法。

6. 根据权利要求 5 所述的装置，其中所述加密器被设置为使用一个加密密钥，并且该电路被设置为从所述参数导出所述密钥。

7. 根据权利要求 1 所述的装置，其中所述参数是电参数。

8. 根据权利要求 1 所述的装置，其中所述参数是磁性参数。

9. 根据权利要求 1 所述的装置，其中所述参数是光学参数。

10. 根据权利要求 1 所述的装置，其中所述参数是辐射参数。

11. 根据权利要求 11 所述的装置，其中所述保护部件在基质材料内包括所述电路响应的大量颗粒。

12. 根据权利要求 11 所述的装置，其中所述颗粒是金属性的。

13. 根据权利要求 11 所述的装置，其中所述颗粒是放射性的。

14. 根据权利要求 11 所述的装置，其中所述基质允许辐射通过，并且所述参数是受所述颗粒影响的光学特性。

15. 根据权利要求 14 所述的装置，其中所述颗粒产生辐射。

16. 根据权利要求 14 所述的装置，其中所述颗粒吸收辐射。

17. 根据权利要求 14 所述的装置，其中所述颗粒散射辐射。

18. 根据权利要求 1 所述的装置，其中所述保护部件包括一个结晶体的至少一个去结晶部分。

19. 根据权利要求 2 或 3 所述的装置，其中所述存储器是只读存储器，并且所述电路包括解密器，该解密器被设置为对从其读取的数据应用解密算法。

20. 根据权利要求 2 或 3 所述的装置，其中所述存储器是可写存储器，并且所述电路包括加密器，该加密器被设置为对待写入其内的数据应用加密算法。

21. 根据权利要求 2 或 3 所述的装置，其中所述存储器包括至少一个第一存储器和一个第二存储器，并且所述第一存储器存储对存储在所述第二存储器内的数据进行解密所使用的加密数据，所述电路响应该参数对第一存储器的内容进行解密。

22. 根据权利要求 1 所述的装置，包括窜改检测逻辑电路，它响应一个对该电路的访问尝试产生窜改信号。

23. 根据权利要求 1 所述的装置，其中该电路联合地响应所述物理参数和预定的保密加密数据来应用加密过程和/或解密过程。

24. 根据权利要求 23 所述的装置，包括窜改检测逻辑电路，它响应一个对该电路的访问尝试产生窜改信号。

25. 根据权利要求 24 所述的装置，其中该电路被设置为响应该窜改信号来删除预定的保密加密数据。

26. 根据权利要求 1 所述的装置，进一步包括围绕该保护部件的屏蔽，该屏蔽被设置为降低外部条件对物理参数的影响。

27. 根据权利要求 1 所述的装置，进一步包括至少一个响应所述保护部件的传感器，所述电路通过该传感器导出所述至少一个参数。

28. 根据权利要求 27 所述的装置，包括多个用于检测所述至少一个物理参数的传感器。

29. 根据权利要求 28 所述的装置，其中所述传感器以阵列形式被设置在至少部分所述电路上。

30. 根据权利要求 29 所述的装置，其中传感器之间的间隔在微米数量级。

31. 根据权利要求 28 所述的装置，进一步包括扫描电路，被设置为周期性读取所述传感器。

32. 根据权利要求 31 所述的装置，其中所述扫描电路被设置为改变读取所述传感器的顺序。

33. 根据权利要求 31 所述的装置，进一步包括校验电路，被设置为校验所述传感器的输出是否与其先前的值一致。

34. 一种集成电路装置，包括：存储器，以加密形式存储数据；以及电路，用于进行加密和/或解密以写入和/或读出数据，该电路包括：密钥寄存器，用于存储所述加密过程和/或解密过程中使用的密钥；以及交替电路，被设置为以频繁间隔改变存储在密钥寄存器内的数据。

35. 一种访问存储在存储器装置内的被加密的数据的方法，包括从一个阻挡对电路的访问的保护部件导出加密数据，以及利用所述加密数据访问所述被加密的数据。

集成电路的防窜改封装

技术领域

本发明涉及防止存储在集成电路组件（例如电集成电路或计算机芯片）中的存储器内的保密敏感内容（例如：数据、程序或密码信息）被窜改的装置和方法。这种集成电路的例子有：例如电子银行、自动提款机、收费电视、移动电话等中使用的智能卡、微控制器、微处理器或 ASIC。

背景技术

已知有多种方法可以防止集成电路被窜改。一种方法是致力于研究封装材料；例如，通过附加玻璃颗粒来防止用机械方法磨掉涂层。然而，研究发现，任何一种芯片外壳都可以利用某种方法（例如：酸、碱、溶剂、等离子体或活性离子腐蚀剂、聚焦离子束、激光或机械研磨）被攻击，并且针对这些方法中的某种方法对封装进行改进后会使得更难以抵抗其它方法的攻击。US 5369299 披露了一种防窜改涂层，在这种防窜改涂层中腐蚀覆盖层会破坏有源器件。US 5916944 披露了一种防窜改涂层，在这种防窜改涂层中使用了活性层，它在（被攻击）接触氧气时，发生发热反应以致破坏其下的器件。

另一种方法是利用传感器对窜改芯片进行检测。一旦传感器检测到窜改，就采取某种保护动作。然而，尽管这些方法可以保护有源状态的芯片，但是却不能保护无源状态的芯片。在这种情况下，传感器和控制电路均无效，而且可以除去封装并读取存储的任何数据。

据说 SGS－Thompson 在其芯片表面设置了一层网状保护层。穿透此网状保护层的任何原始尝试都会使电路短路或断路。一旦检测到这种短路，就关闭芯片功能。然而，如上所述，在芯片没有电源时，这种保护也无效。US 5861662

披露了一种类似技术。

某些智能卡制造商采用的一种完全不同的方法是，对芯片内容“加扰”。例如，利用芯片上的加密/解密单元，Philips Visa 卡和 Siemens SLE66C160S 银行卡对其存储数据提供内部内容加扰（加密）。

现在，即使“黑客”或“掠夺者”（以下会互换地使用这些术语，他们表示任何试图进入的未授权个体）试图从芯片存储器内读取数据，由于数据被加扰，为了将数据转换为解密形式或“明文”形式，他必须反向设计（reverse engineer）芯片上的加密/解密单元并且还要知道加密密钥。

然而，由于为了对数据解密，芯片本身必须保持加密密钥，所以对于精明的黑客来说，此操作是可能的。

在“Design Principles for Tamper Resistant Smart Card Processors”公开于 proceedings of the USENIX Workshop on Smart Card Technology(10-11 May 1999)和“Low cost attacks on tamper resistant devices”, Security Protocols 5th International Workshop Proceedings, 1997 p125-136 内对各种攻击以及防止攻击的技术进行了说明。

发明内容

本发明试图提供一种用于防止电路组件（例如：集成电路、半导体芯片）中的存储器的内容被窜改的改进型装置和方法。

根据一个方面，本发明提供了一种利用解密器访问以加密形式存储的数据的集成电路装置，以及一种可以减少对电路的访问的保护部件（例如：封装或包装），其特征在于，电路采用的加密过程响应于保护部件的至少一个物理参数，并设置保护存储器，这样在进行窜改以访问电路时会改变物理参数，使得加密过程以不同方式工作。

根据另一个方面，本发明提供了一种访问以加密形式保存在集成电路装置内的数据的方法，该方法包括从用物理方法阻挡对电路访问的保护部件导出加

密数据（例如：密钥）的步骤。

通常，保护部件是电路上，和/或围绕电路的一个层，例如封装层。

根据又一个方面，本发明包括一种电路，该电路具有实质上封闭该电路的封装，并以这样的方式设计该封装，即它参与电路的密码保护过程，以致如果封装被扰动，电路就不实现正常功能。

因此，因为从保护层本身获得对加密或解密必不可少的数据，所以通过除去保护层来到达其下的电路的任何尝试均会破坏解密保存在电路内的内容所需的数据（例如：密码算法的密钥）。

通过提供此保护层，由部件（例如：涂层）的物理参数导出密钥，而非（例如）将它们保存在其内的寄存器内，所以不可能通过去除涂层来在中途读取密钥值。

优选从在集成电路上或围绕集成电路散布的保护部件区域内检测、获得一个或多个物理参数。因此，例如，物理参数可以是体参数或面参数，或者从大量的不均匀断续性（诸如分散颗粒）获得该物理参数。

在这种情况下，可以防止通过保护部件钻小孔（例如以读取芯片的地址线或数据线）的各种尝试，因为在体特性或面特性的情况下，每当钻这种孔时都会改变该参数；并且在分散断续性的情况下，各检测区域之间的间隔是所钻最小孔宽度的数量级。

在各装置之间，物理参数优选是无序或随机的，这可能是无序或随机的制造过程（例如：不确定不均匀性的位置）的结果。因此，对于每个装置，加密数据（例如密钥）是唯一的而且只有该装置知道，这样就不可能从中央信息源偷取加密数据用于所有装置，或者说不可能击败一个装置的保护，然后把加密数据用于另一个装置。

因此，在此实施例中，电路具有这样的初始化模式，即读取该参数，并根据参数值首先对保存在该装置上的数据进行加密。

在一个实施例中，将内容保存在可电改写存储器内，因此允许以加密方式

重写它。

在另一个实施例中，以第一加密形式，将所有装置上的数据保存到一个存储器（可以是不可改写存储器，例如掩模编程 ROM）内。第一加密形式是预定的，并且与保护存储器无关。第一加密过程的密钥保存在一个可改写存储器内（例如可电改写存储器），并且在初始化过程中，以第二加密形式对此密钥进行加密，第二加密响应于该物理参数导出，并以该形式存储到可改写存储器内。此后，为了从 ROM 读取数据，利用第二密钥对第一密钥进行解密，然后利用第一密钥对数据进行解密。

此外，或者另选地，为了确保各装置之间的加密数据不同，从具有大公差（即，在此情况下，是指制造传感器过程中具有规定的低精确度）的一组传感器中对不同装置选择一个或多个传感器，因此在各装置之间，对于给定参数值，传感器读数将不同（尽管对于给定装置在时间上是稳定的）。

因此，即使可以准确测量传感器检测的物理参数值，传感器对其的响应（因此加密数据）也不是明显的。

构成保护部件（例如：封装）的体或面的材料优选是不均匀的，并且在每个装置内不均匀性分布优选是无规则或随机的，因此通过仅对部分保护存储器进行研究，不可能预测物理参数。

上述说明的实施例可以有效保护芯片在未加电时免受攻击。此外，为了在加电情况下也保护芯片，需要采取附加措施。例如，可以以较频繁间隔（比穿孔或去除保护部件所需最短时间更频繁地）从保护部件扫描物理参数。在注意到数值发生变化时，就采取行动删除保存在芯片上的保密内容（即：被加密的数据），否则就象在现有技术中那样，禁止芯片工作。

优选以波动形式（例如：被翻转或被循环）保存从物理参数导出的加密数据，因此可以避免基于对缓存加密数据的存储器进行“冻结”的攻击。

存在这样的可能性，即通过保护部件钻小孔仅破坏部分加密密钥，而攻击者可以利用其它可用部分进行读取，因此，攻击者可能进行“强力”攻击以破

图 5A 示出磁性传感器实施例的简化示意图；

图 5B 示出取自在线 VB－VB 的、图 5A 所示装置的剖视图；

图 6 示出第一电传感器实施例的示意图；

图 7 示出第二电传感器实施例的示意图；

图 8A 示出电容性传感器实施例的示意图；

图 8B 示出取自线 VIIIB－VIIIB 的、图 8A 所示装置的剖视图；

图 9 示出优选实施例的密钥翻转寄存器的方框图；

图 10 示出根据另选实施例构造和操作的电路组件方框图；

图 11 示出图 10 所示装置的一个可能实现的剖视图；

图 12A 示出根据另选实施例构造和操作的封装电路组件的示意图；

图 12B 和图 12C 分别示出侵入性切开图 12A 所示装置的动作及其效果的示意图；

图 13A 示出另一个实施例的示意图；

图 13B 是图 13A 所示装置一部分的剖视图，示出了侵入性切开图 13A 所示装置的动作及其效果；

图 14 是说明第一实施例完成的初始化过程的流程图；

图 15A 是说明装置操作过程的流程图；

图 15B 是更详细说明该过程一部分的流程图；

图 16 是说明采用两个存储器的本发明进一步实施例的方框图；

图 17 是说明采用成对密钥的本发明进一步实施例的方框图；

图 18 是更详细说明该实施例一部分的方框图；以及

图 19 是更详细说明该实施例另一部分的方框图。

第一优选实施例的说明

图 1A 示出第一实施例的简化方框图。

图 1A 所示的装置包括中央处理单元（CPU）100，它可以是一个标准 CPU

解加密过程。在一个实施例中，为了防止出现这种情况，提供一个随机密钥并存储在电路内，并且如上所述，从保护部件读取第二密钥。作为这两个密钥的联合函数（例如：诸如 XOR 组合的逻辑组合），产生用于加密或解密数据的解密密钥。

如果扫描操作指出丢失了从物理参数导出的部分或全部密钥，则该电路删除存储在其内的随机密钥。因此，即使黑客重构了从保护部件导出的密钥的剩余部分，仍不能重构用于解密所存储内容（其是现在删除的随机密钥和从保护部件导出的密钥的一个联合函数的结果）需要的实际密钥。

每次扫描优选以随机置换顺序进行，并且作为扫描值的取决于顺序的函数产生加密密钥。因此来自传感器的扫描序列的顺序并不对应于用于计算加密密钥的传感器值的顺序。因此，在因为受到攻击而丢失扫描值的某些位的情况下，攻击者不可能发现丢失的位位于用于产生解密密钥的序列内的什么位置。这样就显著提高了对密钥进行强力攻击的难度，因为尽管知道序列的剩余位，但是不知道它们的顺序。

物理参数（从广义上说，用于表示要检测的任何特性）可以是光学参数、电参数、磁性参数或从大量其它可能范围中选择的参数，以下将做更详细说明。

根据以下说明和权利要求，本发明的其它实施例、优选特征以及相应优势将变得更加明显。

附图说明

现在，将仅利用例子，参考附图说明本发明实施例，附图包括：

图 1A 示出根据本发明第一实施例构造和操作的电路组件方框图；

图 1B 示出图 1A 所示装置的一部分的优选实现的方框图；

图 2 示出图 1B 所示装置的加密部分的优选实现的方框图；

图 3 示出图 1B 所示装置的传感器电路部分的优选实现的方框图；

图 4 示出图 1B 所示装置的传感器布局的优选实现的示意图；

核心，例如：Motorola 6805/8051/6811 或 Intel 8051。

该装置进一步包括非易失性（NV）存储器 110，在此实施例中，非易失性存储器 110 是可改写的（例如，它是 FLASH 或 EEPROM 或铁电随机存取存储器（FERAM））。存储器 110 包括存储保密数据内容的存储区，其内容对黑客保密，例如，保密数据内容包括：口令、密码密钥数据、加密或解密程序、数字签名程序或数字签名验证程序。

此外，还提供了加密/解密单元（EDU）120。通过利用 EDU 120 发送读写请求，CPU 100 访问存储器 110。例如，EDU 采用本技术领域内众所周知的 DES、3DES、IDEA 或 TEA 加密算法，或任何其它合适的密码算法。

利用密码输入单元 130 提供的加密密钥 160，加密/解密单元 120 进行加密和解密。利用相应多个传感器 150 输出的多个检测特性输出 140，密码输入单元 130 可操作地形成密钥 160，传感器 150 响应于围绕电路的封装 50 的封装特性 170。

现在，需要参考图 1A 对此实施例的操作过程做个总结。在操作过程中，传感器 150 检测参数 170 的各个值，并产生相应的检测特性输出信号 140，密码输入单元 130 对这些检测特性输出信号 140 进行组合以提供密码输入（密钥）160。将密码输入 160 送到加密/解密单元 120。至少在每次对芯片加电时，并且（在此实施例中）在接通电源期间以规则间隔，进行扫描传感器和提供密码输入 160 的操作。

CPU 核心 100 从存储器 110 请求连续程序指令和数据。不是将每个请求送到存储器 110，而是将每个请求送到加密/解密单元 120。选择存储器 110 的地址线后，将加密形式的内容（程序或数据）字（190）从存储器 110 送到加密/解密单元 120。加密/解密单元 120 对加密内容字 190 进行解密并将相应解密字或明文字送到 CPU 核心 100 进行处理。加密/解密单元 120 在 CPU 100 与存储器 110 之间的操作实际上是透明的。

在封装 50 被窜改时，封装特性 170 发生变化，从而导致检测特性 140 以

致密码输入（密钥）160发生变化。因此，加密/解密单元120不再正确解密来自存储器110的程序和/或数据，并且CPU核心也不再正常操作。

现在，将参考图1B进一步详细说明此实施例。在此实施例中，所制造的集成电路或微芯片195包括：CPU核心100、存储器110、加密/解密单元120、密码输入单元130以及传感器150。捕获逻辑电路197（图1A内未示出）捕获传感器150输出的检测特性信号140。

此外，还提供了输入/输出电路210，它与接触焊盘（未示出）相连，接触焊盘使电路195连接到外部装置。接触焊盘可以进行连接以使被封装的装置用于诸如读卡器的其它装置。在此实施例中，接触焊盘还在制造该装置之后，允许连接到诸如探针焊盘的测试装置。最后，提供初始化电路200。初始化电路包括用于存储装载程序的只读存储器（ROM），装载程序包括用于装载初始密钥的第一部分，以及根据初始密钥以第一加密形式加密的第二部分。

参考图14，在工厂中进行的初始化过程中，在第一次对芯片加电时，执行装载程序的第一部分，并通过I/O电路210提供初始密钥。利用初始密钥对ROM的内容进行解密，执行装载程序的第二部分。在步骤1002，装载程序读取传感器150输出的检测特性信号140。在步骤1004，根据检测特性信号140，捕获逻辑197和密码输入单元130产生密钥。

接着，装载程序执行一个循环，在该循环中，在存储了存储器110的保密数据存储区内的所有保密数据之前（步骤1012），在步骤1006，从I/O电路读取一个数据字，在步骤1008，加密/解密单元120对数据字进行“即时”加密，在步骤1010，将该数据字写入存储器110。

最后，在步骤1014，装载程序使初始密钥被删除，将加密形式的装载程序第二部分保留在初始化电路内以避免该电路的重新初始化。由于只有制造商知道初始密钥，所以其它人不可能使用装载程序的第二部分，而且除非知道初始密钥，否则第一部分没有价值，因为装载任何其它密钥均不能对装载程序的第二部分进行解密。

顺便提一下，请注意，在公知的加密电路装置内也可以使用这种禁止装载程序的过程，而不象在本实施例中那样使用从封装导出的加密原理。

因此，在执行了图 14 所示的初始化过程后，只有利用密钥 160 通过加密/解密单元 120 进行解密，才可以访问存储在存储器 110 内的保密内容数据。

此外，或另选地，不是通过输入/输出单元提供所有数据作为一个数据流，而是，首先以明文形式将它送到存储器 110 内，然后在初始化期间被重写。

该装置的操作过程

参考图 15A，在使用时，接通电源后，在步骤 1102，电路被设置为读取检测特性数据 140，并如以前一样在步骤 1104 形成一个密钥（对应于上述步骤 1002 和 1004）。在步骤 1106，该装置执行其操作循环，以下将参考图 15B 说明此操作循环。当在步骤 1108 切断电源时，加密/解密电源 120 和密码输入单元 130 内的寄存器被刷新以清除该密钥。操作过程结束。

参考图 15B，在操作过程中，根据从输入/输出电路接收的信号（例如：指示进行读数据或写数据），CPU 100 执行其操作程序。

在步骤 1202，加密/解密电源 120 检测 CPU 100 何时要执行对存储器 110 的保密存储区的读指令或写指令。如果该指令为读指令，则在步骤 1204，从存储器 110 接收相应字，在步骤 1206 解密，并在步骤 1208 送到 CPU。

如果相应指令是写指令，则在步骤 1214，EDU 电路 120 接收 CPU 100 输出的数据字，对它进行加密（步骤 1216）并将它写入存储器（步骤 1218）。

完成步骤 1208 或步骤 1218 后，在步骤 1220，评估是否出现了断电的情况（例如：通过在 CPU 100 上运行一个中断服务例程），并且如果出现这种情况，则停止操作循环 1106。

可以设置 CPU 100 以通过输入/输出电路接受新程序。在这种情况下，作为一种附加的保密特征，该装置被设置为执行一个硬连线复位以在运行新程序之前删除存储器 110 内的所有数据。因此，可以（在工厂内）装载测试程序，

或者利用新初始化程序重新初始化该电路，但是只有在重新提供存储器 110 的内容时才可以，因此黑客不可能提供非法程序以通过 CPU 100 读取或使用存储器 110 内的内容。

现在，将参考图 2 和图 3 进一步详细说明此实施例的优选实现过程。

由 CPU 核心 100 的地址总线（未示出）驱动的传统列解码器电路 210 和行解码器电路 220 对存储器 110 进行寻址。在此图中，将先前附图中的加密/解密电路 120 重新标记为 260，并将密码输入单元 130 的密钥保存寄存器标记为 270。

在此实施例中，第一（字宽）双向锁存器 240 位于 CPU 核心 100 的数据总线与加密/解密电路 260 之间，第二（字宽）双向锁存器 230 位于存储器 210 的数据总线与加密/解密电路 260 之间。在此实施例中，字长度为 8 个字节（64 位）。

混合电路 250 包括与加密/解密电路 260 的输入端相连的双向寄存器，并且混合电路 250 的两个输入端与锁存器 230、240 的输出端相连，因此可以选择性地把数据从一个锁存器或另一个锁存器路由选择到加密/解密电路 260。

同样，分割电路 280（即：双向寄存器）与加密/解密电路 260 的输出端以及锁存器 230、240 的输入端相连。

混合电路 250、分割电路 280 以及锁存器 230、240 均连接到 CPU 100 的读写控制引脚，然而，锁存器 230 和分割器 280 上的倒相器（未示出）使该信号倒相。因此，如果在一个方向使能锁存器 230 时，则在另一个方向使能锁存器 240，反之亦然；并且在控制混合器 250 从锁存器 230 路由时，则控制分割器 280 路由到锁存器 240，反之亦然。

在 CPU 希望从存储器 110 读取数据时，锁存器 230 被设置为从存储器 110 接收数据，并且锁存器 240 被设置为从分割器 280 接收数据；混合器 250 被设置为从锁存器 230 接收数据并将该数据送到加密/解密电路 260，加密/解密电路 260 被设置为对该数据进行解密；分割器 280 被设置为将该数据路由选择到

锁存器 240，锁存器 240 被设置为将该数据送到 CPU 100。

相反，在 CPU 100 要对存储器 110 进行写入时，锁存器 240 被转换为从 CPU 100（的数据总线（未示出））接收数据，并将混合器 250 转换为将数据从锁存器 240 路由选择到加密电路 260 进行加密，并将分割器 280 转换为从锁存器 230 路由选择该被加密的数据，锁存器 230 被设置为将该加密数据送到存储器 110。

在此实施例中，为了读取一个数据字节，CPU 将行地址和列地址放在存储器 110 的数据总线上，数据总线将要求的字转发到锁存器 230。混合器 250 将该字转发到加密/解密电路 260，加密/解密电路 260 对该字进行解密。分割电路（在行解码器 220 的控制下）将解密字转发到锁存器 240，该解密字从锁存器 240 路由选择到 CPU 100。

为了执行写循环，双向锁存器 240 从 CPU 100（的数据总线）接收待写入的字，并通过混合器 250 将该字送到加密/解密电路 260，加密/解密电路 260 对该字进行加密。然后，通过分割器 280，将该字路由选择到锁存器 230，然后再路由选择到存储器 110（的数据总线）。

图 2 所示的加密单元 120 还包括用于执行上述功能的附加控制逻辑电路(未示出)。优选地在自定时逻辑中提供加密/解密电路 120，而非利用 CPU 时钟进行驱动，因此可以比 CPU 操作得更块，从而使加密/解密处理的速度与集成电路的可用时钟速度相同。

为了使加密过程更稳定，优选利用 64 位密钥，以 64 位或更多位数据块形式进行加密（也可以使用更短的数据块，但是保护性差）。

如果利用字长短于 64 位的处理器 100（例如：一个 8 位/1 字节数据总线处理器）执行本发明，则可以对上述实施例做稍许变更，使得始终可以一起对至少 64 位的数据块进行读取和解密、或加密和写入。

在这种情况下，为了读取希望字节的数据，一次从存储器内读取一整个数据列（64 位），并作为一个数据块一起进行解密，然后，利用行地址从其内选择希望字节的解密数据，并转发到 CPU 100 的数据总线。

在这种情况下，为了执行写循环，首先必须执行读循环。因此，读取存储器 110 内的、包括待重写字节在内的整个数据列（由行解码器指出），并转发到加密/解密电路 260，加密/解密电路 260 对其进行解密。然后，从数据总线读取待写入存储器 100 的希望字节，并将它代入解密列。然后，利用加密/解密电路 260 对该列（具有替换的字节）重新进行加密并写回到存储器 110。

参考图 3，图 3 更详细示出传感器 150 以及捕获逻辑电路 197 的结构。

在此实施例中，传感器可以是以下说明的任何一种类型的传感器。通常，每个传感器给出一个模拟输出。将模拟传感器输出连接到双向模拟复用器 290 的各个输入端，地址计数器 295 对双向模拟复用器 290 进行控制。例如，模拟复用器可以是一个 1 至 n 选择器，其中 n 是传感器数量。

在地址计数器 295 的控制下，通过模拟复用器 290 一次一个地将传感器输出的模拟值 140 送到读出放大器 300 的输入，将读出放大器 300 的输出送到模数转换器（ADC）310。利用例如对热敏电阻或其它温度传感器（未示出）响应的公差补偿电路 320 对 ADC 输出进行校正，以根据某个预定校正比例，为温度（或其它环境因数）的效应对每个数字传感器读数进行校正。（当然，如果需要，还可以在进行数模转换之前进行模拟补偿。）

将连续数字传感器读数载入线性反馈移位寄存器（LFSR）330，根据某个加扰函数，线性反馈移位寄存器 330 将它们组合在一起，并利用所有传感器读数，以某种逻辑组合方式，产生要求长度（例如：64 位）的密钥 340。

可以使用的传感器数量多达一百万数量级。因此，最好根据所有传感器读数导出密钥。一种方式是将这些读数相加，或者将特定传感器组（例如，位于阵列的一列上的所有传感器）的读数相加。其结果是一个与组成该组的传感器的扫描顺序无关、但是如果任何传感器输出的值发生变化其也发生变化的总和值。

另一种方式是对每个传感器分配一个一位的值，指出其读数是否超过一个阈值（最初根据读数的统计数字导出）。

图 4 示出位于集成电路芯片 195 顶部的各传感器物理布局示意图（在此将芯片衬底标记为 350）。焊接焊盘 355 使芯片与外部部件通信（例如：通过焊接到其上的引脚）。

所设置的传感器 150 覆盖所有包含电路的区域（或者至少是含有敏感数据或允许访问的电路的所有区域）。在此实施例中，可以将它们设置为一个规则阵列。还将某些传感器 150 设置在集成电路的另一侧（未示出），以防止通过该电路进行未授权访问。通过对希望的行线和列线施加其自身不足（但是组合起来足以超过传感器上二极管的阈值电压）的电流或电压，从而仅激活利用（行、列）地址寻址的传感器，可以通过行线和列线寻址传感器，这非常方便。

然后，利用封装材料封装该装置，封装材料可以是基于环氧树脂并具有不不均匀性的材料，不均匀性的参数由传感器 150 以如下方式检测。每个传感器 150 检测的封装 50 的区域可以互相重叠或邻接；为了防止通过封装钻孔到下面的电路所使用的关键判据是，传感器检测的各区域之间的间隔不大于可以钻的最小孔的宽度（例如：利用聚焦离子束技术）。例如，每个传感器检测几微米的区域。

尽管附图所示的传感器被设置在规则阵列内，但是也可以不按规则设置。可以仅在电路敏感区域上设置各传感器组。

各传感器之间的间隔可以为一微米（10^{-9} m）数量级。因此，要覆盖 1 平方毫米，需要设置 10^6 个传感器。

为了根据本实施例制造该装置，先制造电路和传感器，然后，围绕它们设置适当的封装、其它包装和到接触焊盘 355 的触点。

在公差控制不严情况下，批量生产传感器，因此一个装置的传感器对同一个信号的响应与另一个装置的传感器对同一个信号的响应不同（通常具有不同偏差或增益）。因此，即使黑客可以直接测量参数值，也不能根据测量的参数值直接预测传感器输出。一个装置的传感器响应的测量值也不能用于预测另一个传感器的响应。

同样，为了同样的目的，对每个装置所施加的封装也不同，具体地说，每个装置封装中存在的断续性或不均匀性是随机或是不规则分布的（因此，对装置的一部分进行检验不能用于预测另一部分的特性），并且不同装置之间也不同（因此，对一个装置进行检验不能用于预测另一个装置的参数值）。因此，在制造大批装置时，采用宽松的过程控制。

第二实施例－磁检测

参考图 5a 和图 5b，在此实施例中，传感器 150 是诸如霍尔效应传感器的磁场传感器，它可以包括位于芯片上层开口内的砷化铟薄膜。封装 50 在两侧包围装置衬底 350，并且包括环氧树脂基质 363。在该环氧树脂基质内提供许多不同大小、形状和/或磁导率的颗粒 360。这些颗粒由 Ni-Co-Fe 合金（即：铁素体合金）制成。

在封装层 50 的上、下设置一对板状永磁铁 365a、365b，并通过环氧树脂 363 与封装层 50 接合。以其磁极对准同一个方向的方式设置磁铁 365a、365b，在此实施例中，该方向方便地垂直于板 365。

围绕板 365 和封装 50 的是软磁芯材料的外壳 370。外壳 370 的作用是将磁场大致限定在外壳内，并且将该磁场与外部磁场隔离。它具有适当的高磁导率（发现在 10^3 至 10^6 之间合适）。如图 5b 所示，颗粒 360 的作用是使磁力线变形。因为颗粒 360 分布的非均匀性，磁力线的形状不规则。

因此，传感器 150 在每个传感器测量的磁特性不同，如上所述。

此外，去除外壳 370 的任何尝试本身均会改变磁场分布，因此不可能读取密钥。

在另一种磁设置中，利用随机分布的铁磁颗粒的（高）磁导率的局部变化可以改变包括传感器 150 在内的相交引线的感应率。

第三实施例－水平电阻检测

图 6 示出其中利用封装的电阻率的局部变化产生密钥的实施例的结构。

在这种情况下，传感器 150 包括与封装 50 接触的导电开口，并且该传感器 150 可以单独连接到电压供给线和地线。在使用过程中，传感器之一 381 与电压供给线相连，另一个传感器 383 与地线相连。通过这两个传感器中任何一个（通过测流电阻器提供）的电流提供传感器输出。

在此实施例中，封装 50 围绕该装置的半导体衬底 350。

在环氧树脂基质 363 内，混合具有较高电阻的导电粉，例如：石墨粉。另选地，也可以使用诸如嫁、氧化铜或硒的半导体材料。

此外，非均匀地混合长度、宽度、形状和/或电导率均变化的诸如铜线股的导电颗粒。为了使该装置不受外界干扰，设置外部导电金属壳 390，该外部导电金属壳与环氧树脂基质 363 接合。

因此，在此实施例中，可以测量在任何一对传感器之间通过封装 50 的通路的电阻。由于封装的电阻率因为颗粒 385 的分布发生变化，所以每次测得的此电阻不同。

因为通过封装在该装置上流过电流，所以传感器之间的任何孔均会改变流过的电流，并将改变读数。在这种情况下，可以将每个点的传感器输出读数方便地计算为从该传感器流入其每个相邻传感器的测量电流之和，因此衬底上的一个点（以及位于其上的封装）将位于几个传感器所响应的区域内（即：相邻传感器检测的封装区域重叠）。

在此实施例中，温度变化会导致电阻率波动，因此在进行数字化之前，在一个减法节点，取各对电阻测量值（分别位于一对传感器之间）之间的差值。这样可以降低温度效应。另选地，也可以使用比值，或者任何其它差分测量值。

第四实施例－垂直电阻检测

除了提到的差别之外，此实施例与上一个实施例的结构大致相同。

在此实施例中，在外壳 390（如果此实施例要求，可以省略）内，设置与

封装 50 电接触的、例如铝制的内部导电层 391，并且内部导电层 391 还与集成电路的地线引脚相连。

在此实施例中，通过测流电阻器，每个传感器 150 可以选择性地连接到电源线。为了读取每个传感器 392、394、396、398 正上方的封装路径的电阻，它们分别依次连接到电源线，通过每个路径的电流流过传感器和封装到达接地金属层 391，利用测流电阻器测量该电流。以此方式，一次扫描可以逐次测量传感器 392、394、396、398、400 的电阻 R1－R5。此外，优选采用差分测量。

第五实施例－电容性检测

图 8a 和图 8b 示出采用电容性传感器的实施例。在此实施例中，每个传感器仅包括：接触焊盘，位于用于阻挡直流通过的绝缘材料层 410 下方；以及电路，用于施加交流电压并用于测量通过此接触焊盘的电流。

如上所述，层 405 接地。在此实施例中，层 390 是外部保护外壳。在树脂 363 内设置许多颗粒 411。这些颗粒可以在局部改变封装 50 的介电常数。

在此实施例中，通过每个传感器 150，模拟复用器施加具有快速变化分量（即交流分量）的信号。例如，通过在 0 伏与电源电压电平之间快速改变传感器 150 获得这样一个信号，从而在传感器 150 与上层 390 之间产生一个具有交流分量的信号（绝缘层 410 阻挡直流分量）。

例如，利用上述测流电阻器，测量通过传感器的电流（并因此测量传感器之上的材料的电容）。

第六实施例－密钥保存寄存器

现在，参考图 9，说明密钥保存寄存器的结构，该密钥保存寄存器适于防止通过利用辐射过程或冷冻过程冻结密钥寄存器进行的攻击。

二对一复用器 602a、602b、...602e 的输入阵列分别在第一输入端接收该密钥的 1 位。在这种情况下，存在 64 个这种 2 位复用器。

每个复用器 602 的输出到达一排 D 型触发器 604a、604b、...604e 中相应一个触发器的数据输入端。每个触发器 604 的正常（即：未倒相）输出端到达第二排二对一复用器 606a、606b、...606e 中相应一个二对一复用器的第一输入端。

因此，利用第一复用器、D 型触发器以及第二复用器，可以对密钥中每位的值进行计时。

将每个触发器 604 的复位输入端连接到一个 OR 门 608，OR 门 608 接收来自 CPU 100 的复位线以及来自保密故障检测器（未示出）的输入。因此，在 CPU 100 被复位时，或者在检测到保密故障时，将复位触发器以删除密钥。

将每个触发器的倒相输出送到相应第二复用器 606 的第二输入端和相应第一复用器 602 的第二输入端。

从另一个双向复用器 610 提供信号到每个 D 型触发器的时钟端，双向复用器 610 的第一个端口接收 CPU 时钟信号，其第二个端口接收一个随机时钟信号。因此，通过触发器以随机间隔对数据进行计时，可以防止任何利用辐射光源每秒时钟周期的频闪脉冲读取密钥的尝试。

一个根据芯片被设置为装载数据还是执行 CPU 程序来改变其状态的装载/运行线选择每个第一复用器 602 的两个输入端中哪个输入端被路由选择到其输出端。

另一个触发器 612 的复位线与 OR 门 608 的输出端相连，其输入端与复用器 610 的输出端相连，其输出端与复用器 606 的控制输入端相连，从而选择两个输入端中的一个输入端被路由选择到其输出端。因此，对于每个时钟周期，触发器 612 在这排 D 型触发器 604 的真实输出端与倒相输出端之间交替一次。

其效果是，对于每个（随机）时钟周期，翻转触发器的寄存器内密钥的每位，而将该密钥保持在这排第二复用器的输出端供加密/解密使用。

第七实施例－分离的芯片

在上述实施例中，本发明的保密特征集成在具有 CPU 核心和存储器的单个集成电路芯片内。图 10 示出允许本发明使用分离的集成电路的实施例。

在此实施例中，与单独非易失性存储器芯片 460 一起提供单独 CPU 或微处理器单元芯片 470。在此实施例中，存储器是可写入的，例如 FLASH 或 EEPROM，如上所述。

位于存储器 460 与 CPU 470 之间的是与 CPU 470 和存储器 460 的地址总线和数据总线相连的集成电路 450，集成电路 450 含有本发明的保密特征。将它们三个设置在一个公共印刷电路板 485 上（如图 11 所示）。

在此实施例中，传感器 150 分布在印刷电路板 485 之上，并通过导线连接到集成电路 450。将它们设置在印刷电路板 485 的两侧并且还设置在集成电路 450 上。

围绕 PCB 485，在其两侧是含有特征 385 的封装 50，特征 385 可以是上述任何一种类型，适于被传感器 150 检测。

在将芯片 450、460、470 放置在 PCB 485 上之后，围绕它们设置封装 50，并添加引脚以提供电接触。最后，添加保护外壳 480 以避免封装 50 被意外损坏。

与在上述实施例中相同，在工厂对装置进行初始化，在初始化过程中，通过 I/O 接口将数据送到该装置，然后，利用由封装 50 导出的密钥进行加密，并将该其存储到存储器 460。

根据上述说明可以明白，在此实施例中，除了存储器 460 和 CPU 470 之外，电路 450 含有上述实施例中的所有部件。

因此，此实施例使得本发明可以与传统或第三方存储器和 CPU 芯片产品一起使用，而无需对它们做重大调整。

第八实施例－自毁涂层

图 12A 至图 12C 示出一个实施例，在该实施例中，除了在上述实施例中说

明的大量随机分布的特性调整颗粒之外，封装 50 还含有许多微囊体，该微囊体内含有一种或多种封装物质（即液体形式的）。例如，可以提供第一和第二种不同物质 500 和 510 的囊体，它们在接触时一起发生反应以产生链式反应，此链式反应使其它微囊体破裂。

图 12B 示出试图用机械方法打开芯片封装的情况，图 12C 示出结果是囊体 500 和 510 破裂并互相接触，引发一个两部分放热反应，该放热反应使其它封装破裂，从而传遍整个封装 50。这样会使传感器 150 测量的参数发生实质变化，从而销毁加密密钥。

应该以这样的方式进行封装，即在正常处理情况下，封装区域不破裂，但是在试图接合或侵入封装 50 内时，会非常容易地发生破裂。仅要求封装被实质地改变，而不要求下面的芯片也被破坏。

第九实施例 - 光传感器

参考图 13A 和图 13B，在此实施例中，封装或包装材料 50 由诸如聚合物（例如：环氧树脂、聚丙烯）或碱金属硅酸盐（例如：$NaSi_4$）的光透射基质 515 制成。它还可以包括光透射结晶体（例如：结晶聚合物）。

此外，还设置了至少一个光源 520（图 13A 示出多个光源），它位于集成电路 350 的表面上。光源可以方便地是发光二极管（LED）。在此实施例中，传感器阵列 150 是光传感器。

聚合物封装 515 包括大量随机分散的颗粒 530，颗粒 530 与光源 520 发出的光互相作用。这些颗粒会折射、反射、衍射或吸收光。光源发出的光在传感器 150 的阵列上产生干涉图，干涉图就是颗粒分布特征，并且用于产生上述密码密钥。例如，这些颗粒可以是小晶粒。

在基质包括结晶体的情况下，它可以包括许多去结晶区（decrystallised areas）以起到颗粒 530 的作用。可以以公知方式，利用聚焦激光束来产生去结晶区。

在此实施例中，封装 50 优选被接合在其上的硬质外壳 540 完全包围，外壳 540 的内部反射光，并且不允许外部的光进入到其内部。因此，传感器 150 检测的光不会受到外部光照条件的影响。

由于硬外壳 540 的反射作用，所以干扰或去除涂层的尝试会导致传感器 150 检测的光发生变化。

在操作过程中，光源 520 发出多种光束。到达封装 50 外表面和外壳 540 内表面的光束（例如：光束 560）被反射回内部，并最后到达传感器之一（标记为 565）。

图 13B 示出侵入性打开该装置的结果。这将产生一个开口 570，使诸如光束 560 的光束通过开口 570 射出；而不在内部反射。因此，传感器 565 检测的环境发生了变化，所以改变了密钥，因此使得不可能解密。

在此实施例中，每个光传感器方便地分别与一个发光二极管成对配合，并且围绕芯片的外围设置这些光传感器－发光二极管对。来自光传感器－发光二极管对中的发光二极管的光被另一对中的光传感器检测。

第十实施例－只读存储器

在上述实施例中，存储器 110 是可电改写型存储器，因此允许每个集成电路在制造好之后检测其封装的参数并由此导出其唯一加密密钥，然后利用该密钥将数据存储到存储器 110 内。

本实施例使得能够采用只读存储器（ROM），在进行初始化之前，数据以及被存储到该只读存储器内。

参考图 16，可以看到，除了出现了一个附加存储器 111 以及加密/解密单元 120 的操作过程不同之外，此实施例与图 1B 所示的实施例相同。

在此实施例中，存储器 110 是只读存储器（ROM）。以加密形式在只读存储器 110 中提供数据，利用第一预定加密密钥进行加密。之后，以明文形式将第一加密密钥存储到第二存储器 111 内，第二存储器 111 是可写、非易失性存储

器（例如：Flash 或 EEPROM）。

在此实施例中，在进行初始化时，执行图 14 所示的步骤 1002 和步骤 1004。然后，从第二存储器读取预定加密密钥的值（即：解密存储器 110 的内容所需的密钥），然后利用在步骤 1004 产生（即：从封装参数导出）的第二密钥进行加密。然后以加密形式将根据第二密钥加密的第一密钥写回第二存储器 111。

随后，在使用过程中，在每次接通该装置时，第一步骤是读第二存储器 111，并解密从其内获得的第一密钥。此后，读写数据的操作与上述实施例中说明的过程大致相同。在断电时，从保存其的寄存器内删除第一密钥的明文值，在图 9 中，其还进行翻转以挫败冻结攻击。

在此实施例中，用于加密或解密保存在第一（ROM）存储器 110 内数据的密钥并不是以明文形式被永久锁存或保存，所以不可能通过剥落封装进行读取。

对于一组 ROM，第一密钥可以相同，因此 ROM 可以被掩模编程以降低成本。只有从封装导出的密钥加密密钥需要存储在第二存储器内。

第十一实施例－成对密钥

参考图 17 和 18，它们与第一实施例的图 1B 和图 2 以及图 19 对应。

在此实施例中，用相同参考编号表示与上述实施例中的单元相同的单元。

在此实施例中，与在上一个实施例中相同，利用 ROM 110 作为存储器。另外，在此实施例中，采用具有字节宽度（即：8 位宽）数据总线的处理器，具有如上所述 64 位块加密。

另外，在此实施例中，如果不将从封装获得的扫描值直接用于产生密钥来对 ROM 数据的密钥解密，而是将它们与第二数字串组合在一起，则可以改善保密性，以下将该组合称为“成对密钥”，而将扫描值串称为“外壳密钥”。（成对密钥和外壳密钥均不是严格意义上的密钥，因为它们本身不实际用于加密或解密数据，但是成对密钥应当就好象是密钥一样产生）。由此，即使黑客可以

重构扫描值，没有成对密钥，也不可能导出解密数据所需的密钥。

在此实施例中，检测窜改，并且在此检测过程中，删除成对密钥。

显然，此实施例还提供了附加保密，因此特别是可以与物理保密性低的实施例一起使用，但是它在诸如上述磁检测实施例或光检测实施例的实施例中没有必要。

除了上述实施例说明的单元之外，在图 17 中，设置了传感器捕获（或扫描）单元 704，扫描单元 704 扫描传感器 150 输出的、通过传感器总线 708 接收的信号，并将数字捕获信号 718 送到密钥管理单元 702，在密钥管理单元 702 产生进行加密或解密的密钥。

在此实施例中，KSU 704 具有到 KMU 的标准接口，也就是说，它包括用于所使用的任何类型传感器的所有必要部件，并且它将它们的输出转换为标准数字形式。因此，对于不同传感器系统，此实施例装置的任何定制过程均只集中在传感器 150 和 KSU 704。

地址总线 712、数据总线 710、控制总线 706、密钥管理单元总线 716、加密总线 714 以及密钥总线 720 将这些部件互联在一起。控制总线 706 允许 CPU 100 将请求发送到各种其它功能块（KSU 704、KMU 702 以及 EDU 120）。

图 18 示出图 17 所示的、包括 EDU 120 在内的装置部分。具体地说，该图示出 EDU 120、CPU 100、存储器 110 以及密钥保存寄存器之间的关系。

在此实施例中，EDU 120 包括：对称块加密/解密装置（例如，可操作地执行 DES 加密和解密操作）；一对密钥保存寄存器 722、724；列宽度（64 位）双端口明文寄存器 728；以及存储器访问控制（MAC）电路 726（响应地址总线），从保存在两个密钥保存寄存器 722、724 内的两个密钥中选择一个适当密钥，并将它送到块加密/解密单元 260。

与 64 位寄存器 728 的每个字节相连的是相应字节宽度寄存器 730a 至 730h。存储器访问控制电路 726 可操作地选择字节寄存器 730 之一。

参考图 19，密钥管理单元 702 包括传感器地址发生器 801、外壳密钥寄存

器 804、指纹寄存器 808 以及成对密钥寄存器 824。它还包括执行成对功能 822、指纹功能 806 以及比较电路 812 的逻辑电路。

KMU 702 将一个随机数作为成对密钥存储在可擦除寄存器（即：非易失性存储器）824 内。该随机数对于一组装置中的每个装置是唯一的，并且由装载程序在初始化时通过 I/O 电路提供并存储到寄存器内。

第二密钥寄存器 724 内的密钥用于对保存在 ROM 110 内的数据进行加密，在初始化时，通过 I/O 电路提供该密钥并以明文形式将该密钥存储在寄存器 724 内。

在初始化过程中，与在先一个实施例中相同，为了载入外壳密钥，CPU 在控制总线 706 上产生一个信号以使 KSU 704 扫描封装特性。然后，通过传感器总线 708，KSU 从传感器单元 150 接收测量值 802，将这些测量值 802 送到密钥管理单元（KMU）702。密钥管理单元 702 将它们存储到（非易失性、可擦除）外壳密钥寄存器 804 内，与上述实施例相同，外壳密钥寄存器 804 交替该数据以防止“冻结”攻击。

接着，根据外壳密钥寄存器 804 的内容，指纹功能电路 806 计算表征该测量值的“指纹”。指纹功能是一种将测量值以与其顺序无关的形式组合在一起（并且可以方便地是各测量值之和）的功能。将计算的指纹存储到（非易失性、可擦除）指纹寄存器 808 内，在使用该装置的过程中，指纹寄存器 808 始终保存该指纹（除非检测到窜改）。

接着，例如，利用 XOR 组合操作，根据外壳密钥寄存器 804 和成对密钥寄存器 824 的内容计算所要使用的最终密钥，并将它存储在最终密钥寄存器 722 内，最终密钥寄存器 722 保留该最终密钥直到该装置被断电，此时，它将被删除。正如在上述实施例中那样，此寄存器交替该数据以防止“冻结”攻击。如果需要，通过 KMU 总线 716，EDU 访问该寄存器。

最后，根据从寄存器 722 获得的最终密钥，把最初以明文形式存储在寄存器 724 内的、对 ROM 的密钥取出和加密，并以加密形式再存储到寄存器 724，

寄存器 724 保留它直到该装置被断电，此时，它将被删除。该寄存器还交替该数据以防止“冻结”攻击。

在之后每次对装置接通电源时，CPU 100 命令重新捕获传感器值、进行指纹校验、重新计算最终密钥以及重新对 ROM 密钥进行加密。

在该装置正常操作期间，捕获单元 704 较频繁地扫描传感器 150（间隔短于侵入该封装所需的时间，例如每秒钟扫描一次）。在每次新扫描之前，传感器地址发生器 801 计算不同序列传感器读数，这样就可以频繁改变扫描顺序了。但是，虽然它们以不同的顺序出现，每次扫描中的扫描值本身应该相同。

在传感器总线 708 的每次扫描之后，通过将指纹功能 806 应用于外壳密钥寄存器 804 的内容并将此结果与指纹寄存器 808 的内容进行比较，设置 KMU 704 将测量的封装特性与指纹进行比较。

如果不匹配（指示窜改封装），则窜改检测电路 812 将表示报警条件的信号发送到 CPU，CPU 通过控制总线 706 发送报警信号以使 KSU、KMU 以及 EDU 从成对密钥寄存器 824 内删除成对密钥。尽管这本身可能已经足够了，但是还可以删除外壳密钥寄存器 804、指纹寄存器 808 以及加密密钥寄存器 722、724 的内容。

现在简要说明该装置的读写操作，除了下面说明的之外，该实施例的操作方式与第一实施例大致相同。

在字节读循环期间，通过加密总线（64 位宽）714，将包括 CPU 请求的字节在内的 64 位列提供到加密/解密电路 260。如果存储器访问控制电路 726 检测到地址在可写存储器 111 的地址空间内，则选择第一密钥寄存器 722，并将它用于数据解密过程，否则，如果地址位于只读存储器 110 的地址空间内，则选择第一密钥寄存器 722，然后选择第二密钥寄存器 724，并且利用最终密钥对此后用于对数据进行解密的 ROM 密钥进行解密。

块加密单元 260 将解密的 64 位字写入明文寄存器 728。响应放置在地址总线 712 上的行地址部分，存储器访问控制电路 726 选择含有 CPU 100 所请求字

节的一个适当寄存器 730a－h，并使所选择寄存器将该字节载入数据总线 710，从而被 CPU 100 读取。

正如在上述实施例中那样，执行写操作（写入非易失性存储器 111，因为不能写入 ROM）要求首先进行读操作，因为加密的数据块比 CPU 100 使用的数据块大。因此，在明文寄存器 728 内的一列明文可用后（在上述读步骤之后），存储器访问控制电路 726 将待被 CPU 100 写入的字节从数据总线 710 放置到字节宽度寄存器 730a 至 730h 中一个适当字节宽度寄存器内，并重写明文寄存器 728 内相应的 8 位。

然后，利用当前密钥，块加密单元 260 对明文寄存器 728 的内容进行加密，然后通过加密总线 714 将该列写回非易失性存储器 111。

通过与第一实施例进行比较，最容易理解此实施例的作用。在第一实施例中，如果黑客可以对 CPU 100 切割一个小孔，在从理论上说，有可能读出传感器值。钻孔的过程会导致局部特性发生变化，因此少数传感器的读数会发生变化，但是许多其它传感器的读数可能不发生变化。所以通过对几个变化位的所有值进行试验，黑客有可能实现“强力”攻击。

相反，在本实施例中，仅读取传感器输出的参数值无助于推断密钥的剩余位，因为这些位与成对密钥组合在一起了，在检测到窜改时，此成对密钥会被删除。

即使在传感器扫描操作中，黑客可以钻孔并采集数据线上传输的扫描测量值，但是由于扫描顺序发生置换，所以他不知道在测量读数的序列中由哪个读数形成密钥，即应该在哪里设置错误位（受到“强力”攻击的位），因此通过置换扫描顺序，可以提高进行这种攻击的难度。

其它传感器和参数

显然，还可以检测各种其它参数或特性。

在另一个实施例中，辐射也可以用作检测特性。封装 50 的环氧树脂与少

量发出β射线的颗粒（例如：诸如铀的放射性同位素颗粒）混合。

由于这种混合物包围该电路，所以β射线会从芯片的各个侧面到达芯片。传感器是设置在许多位置的β射线检测器（也可以是 x 射线检测器）。该检测器可以接收芯片外壳产生的β射线的复图形。如上所述，任何侵入尝试均会改变从传感器辐射电平产生的密钥。

产生的辐射量低于自然产生的宇宙射线。然而，为了更加安全，芯片外还可以包围某些辐射吸收物质，例如薄铅层，或混合了硫酸钡的环氧树脂层。

在另一个实施例中，可以在层 50 的基质内提供变化的铁电材料颗粒（如铁电 RAM 技术中使用的），并且利用平板电极对层 50 施加电场。利用这些颗粒可以在局部对该电场进行调整，并且与上述电容性实施例中所使用的类似的传感器可以检测到此调整。

在又一个实施例中，利用变化的磁铁电材料颗粒产生一组局部磁场，利用霍尔效应传感器检测该磁场。

还可以使用自旋阀晶体管（spin valve transistor）（可以制造得非常小），而不使用霍尔效应传感器。

无论使用什么样的检测参数，一个理想特征是封装的变化应该在同一个方向影响所有传感器读数。

因此，例如，如果从传感器读数之和导出密钥，则去除封装的尝试无疑会改变密钥值。例如，如果减小封装厚度的影响会提高某些读数并降低其它读数，则从理论上说，该密钥可能保持不变，这是不希望看到的。

其它实施例

尽管对导出密钥的过程进行了说明，但是也可以使用诸如密码算法籽数、密码算法或者它们中任何一个的一部分的密码数据。

尽管对对称加密过程进行了说明，但是，显然，还可以使用非对称加密过程和解密过程。在这种情况下，可以提供不同密钥来进行加密和解密。

尽管在上述披露的实施例中，所示的电路可以进行加密和解密，但是在某些应用中，如果仅从存储器读取数据，则可以在此装置内仅提供解密过程。

尽管对部件和材料的特定例子进行了说明，但是，显然，可以使用任何适当部件和材料，并且说明书内容并不局限于上述部件。

尽管以上对特定加密方法进行了说明，但是本发明并不局限于任何一种这种方法。此外，尽管对采用单独密钥和算法的加密方法进行了说明，但是，显然，只要从围绕该装置的保护存储器的特性导出用于控制加密过程某些方面的数据，则本发明可以应用于任何形式的加密过程。

所采用的电路基于硅材料，或基于诸如砷化钾的 III－V 材料。尽管以上对电子电路进行了说明，但是本发明还可以应用于光电子电路或光学电路或其它电路（例如：分子计算电路）。

尽管对集成电路电路进行了说明，但是，显然，分离部件可以组合为各个分别单独集成的分组合。同样，还可以将本发明的各种部件作为分立逻辑电路实现，或者作为集成专用逻辑电路实现，或者作为在微型计算机或微控制器或 DSP 核心控制下执行的程序实现。

我们认识到，还可以将上述各种实施例的特征组合在一起。请求保护在此披露的任何和所有新颖性内容，而无论它们是否是所附权利要求的主题。

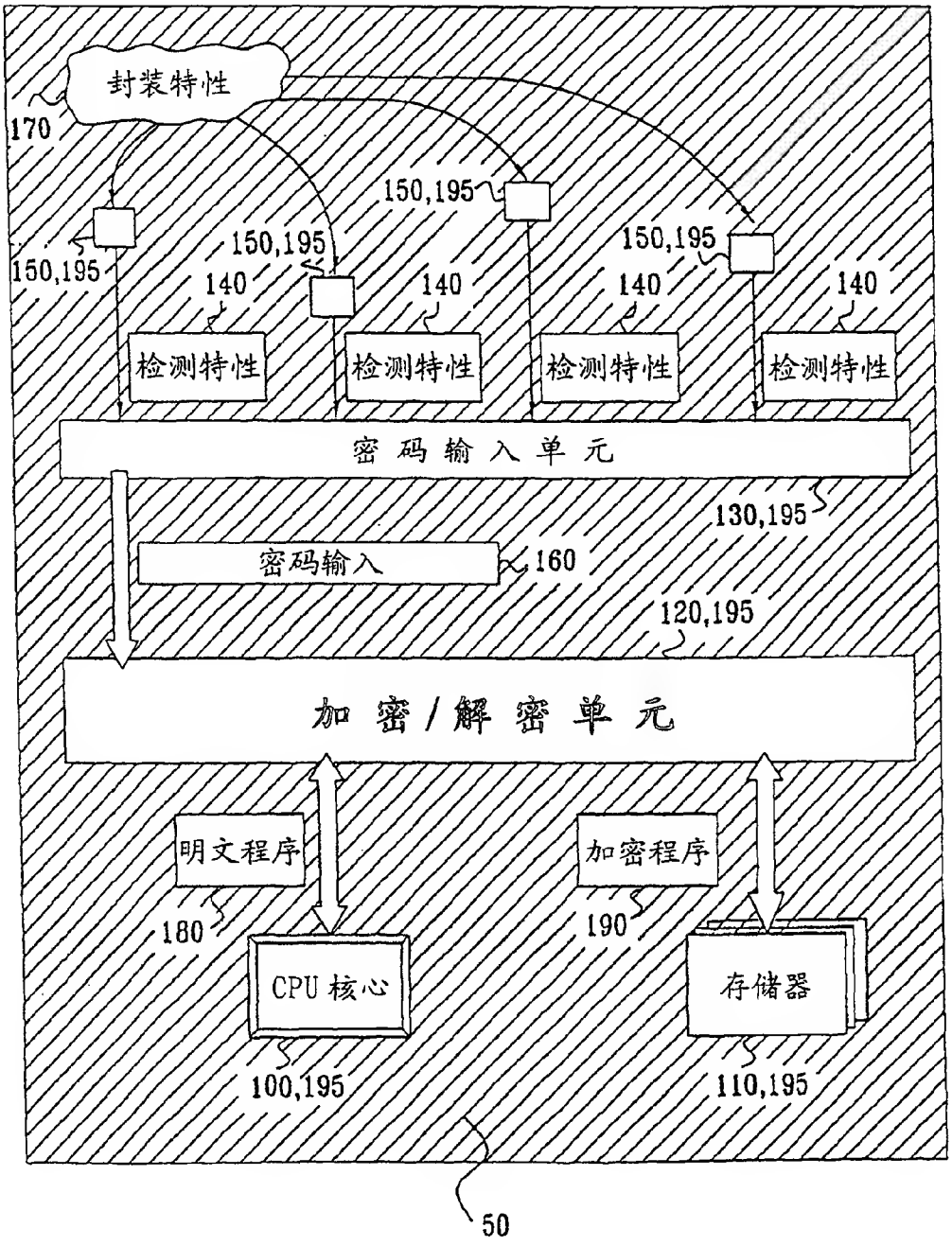

封装特性
170
150,195
150,195
150,195
150,195
140
140
140
140
检测特性
检测特性
检测特性
检测特性
密码输入单元
130,195
密码输入
160
120,195
加密/解密单元
明文程序
加密程序
180
190
CPU 核心
存储器
100,195
110,195
50

图 1A

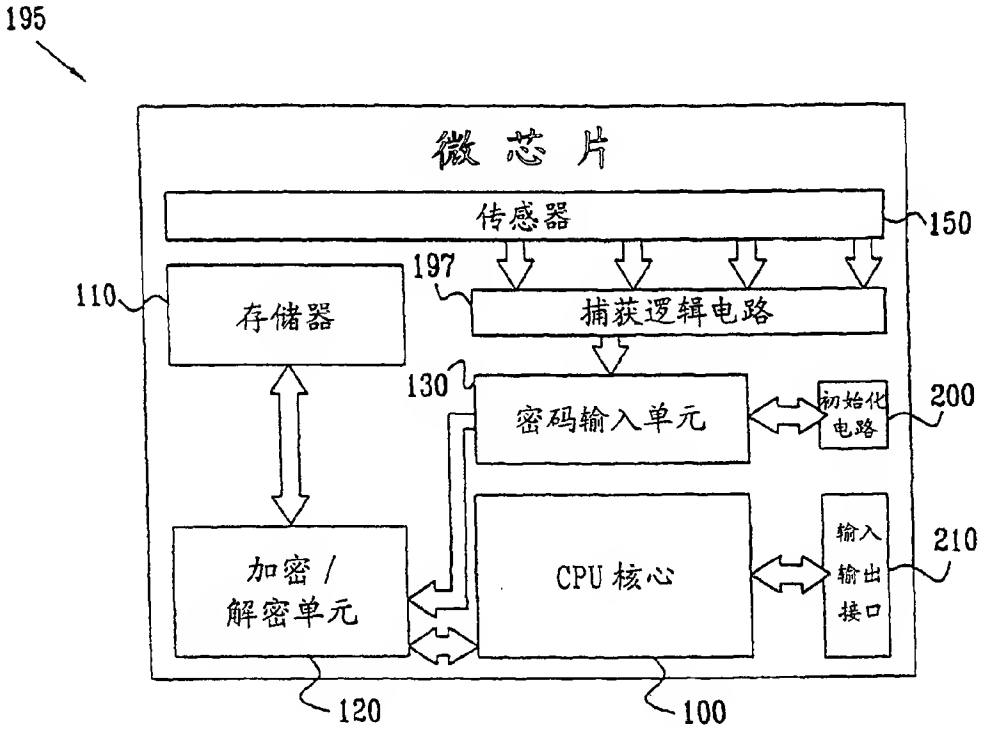

195
微芯片
传感器
150
197
110
存储器
捕获逻辑电路
130
密码输入单元
初始化电路
200
加密/解密单元
CPU 核心
输入输出接口
210
120
100

图 1B

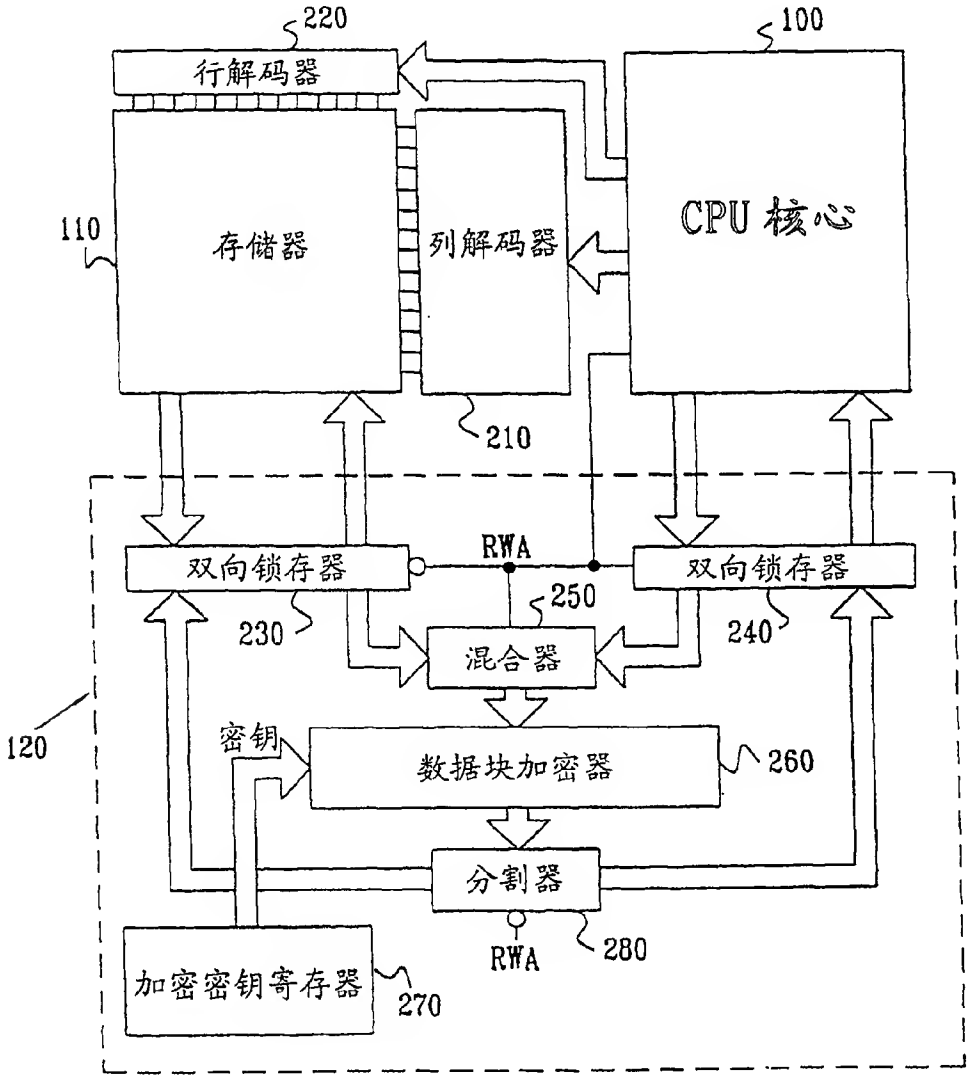

220
行解码器
100
CPU 核心
110
存储器
列解码器
210
双向锁存器
RWA
双向锁存器
250
230
240
混合器
120
密钥
数据块加密器
260
分割器
RWA
280
加密密钥寄存器
270

图 2

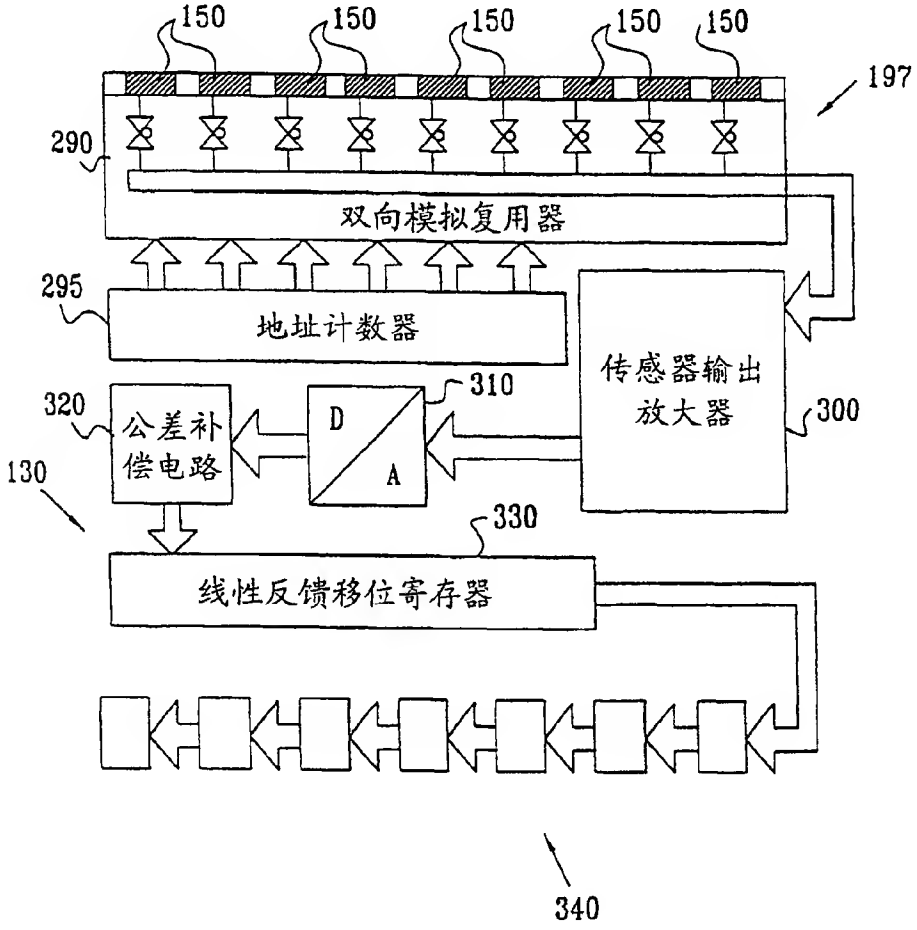

150
150
150
150
150
197
290
双向模拟复用器
295
地址计数器
传感器输出
放大器
300
310
320
公差补
偿电路
D
A
130
330
线性反馈移位寄存器
340

图 3

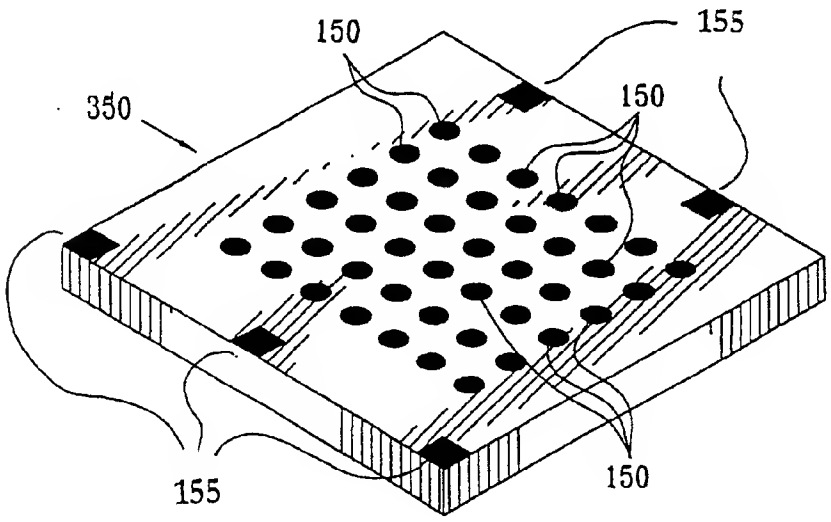


图 4

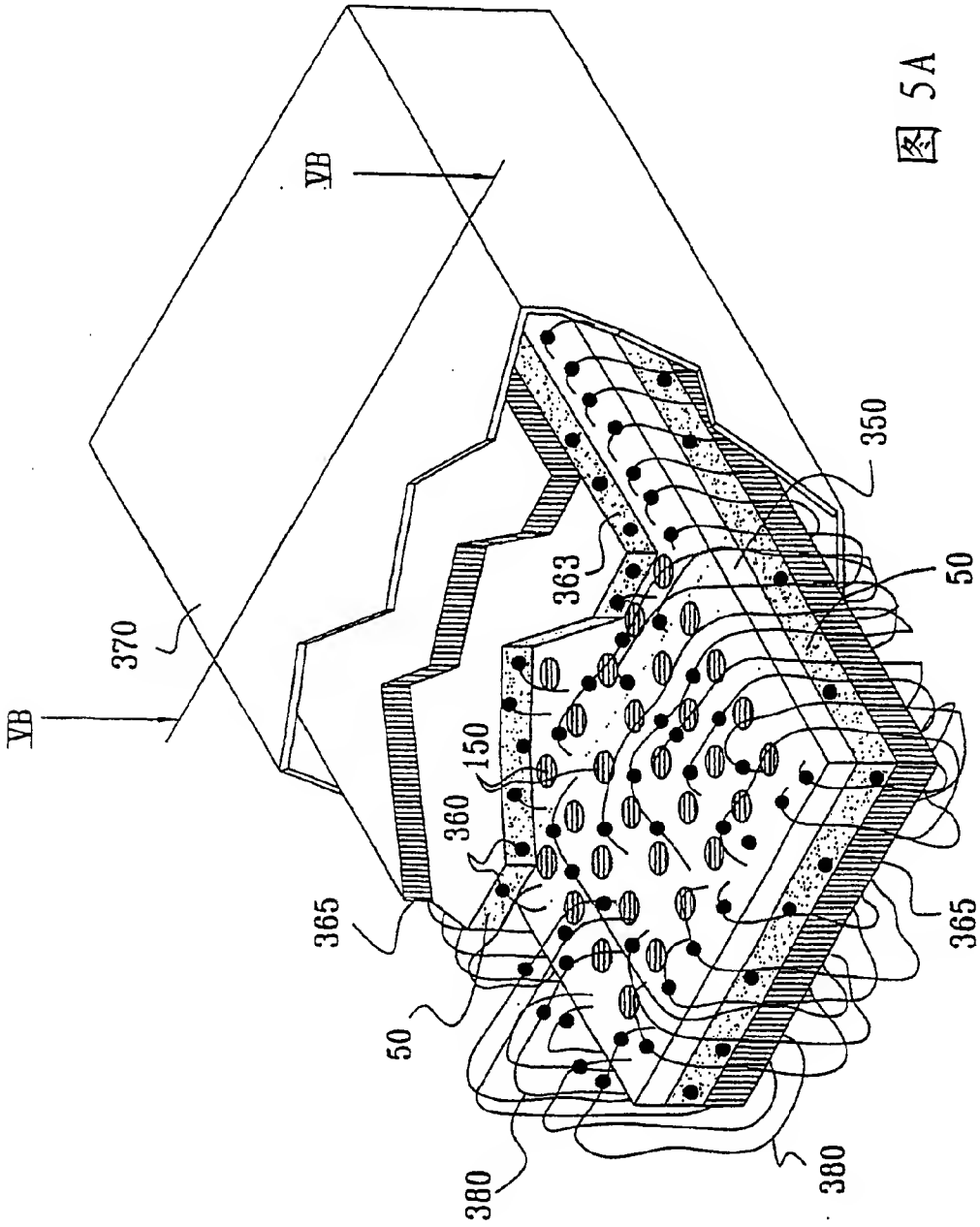


图 5A

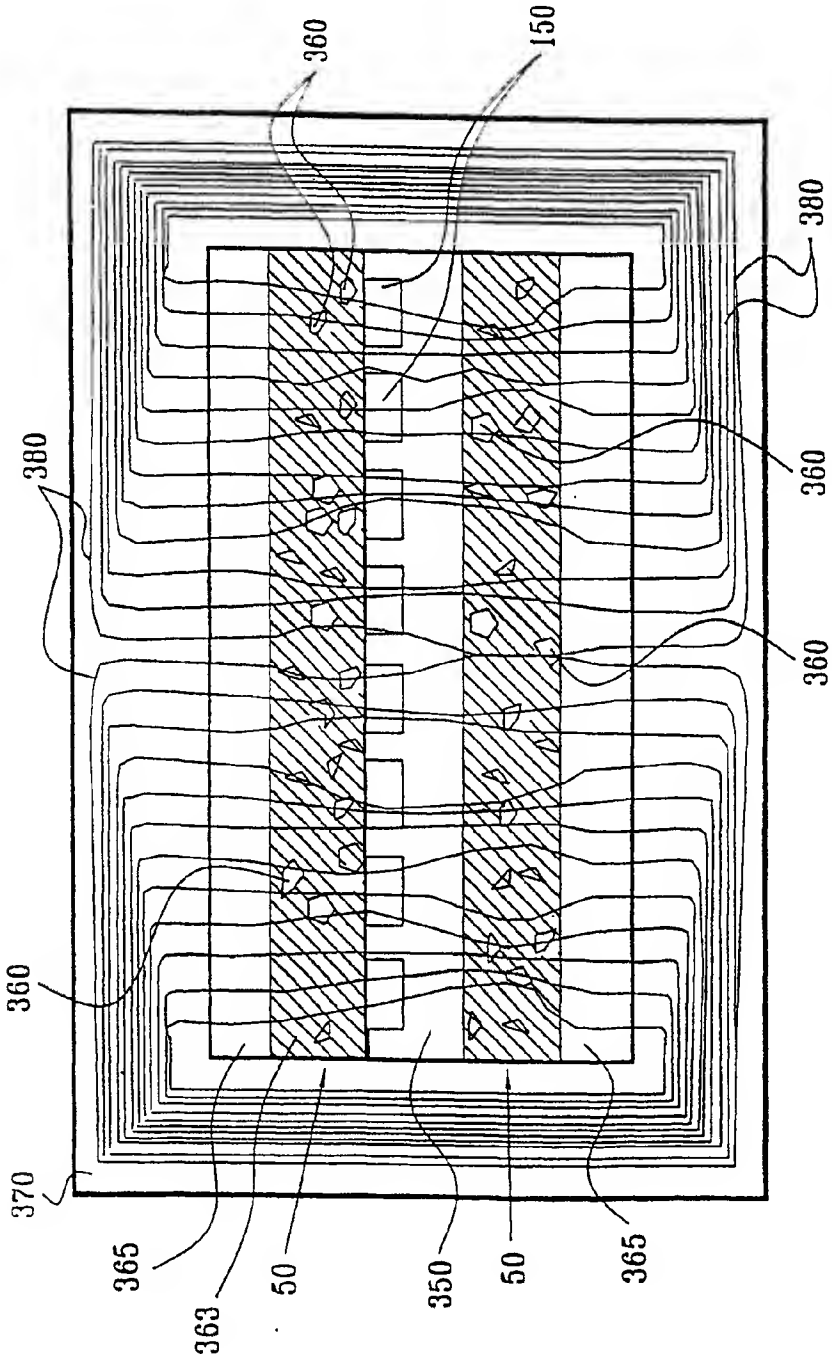


图 5B

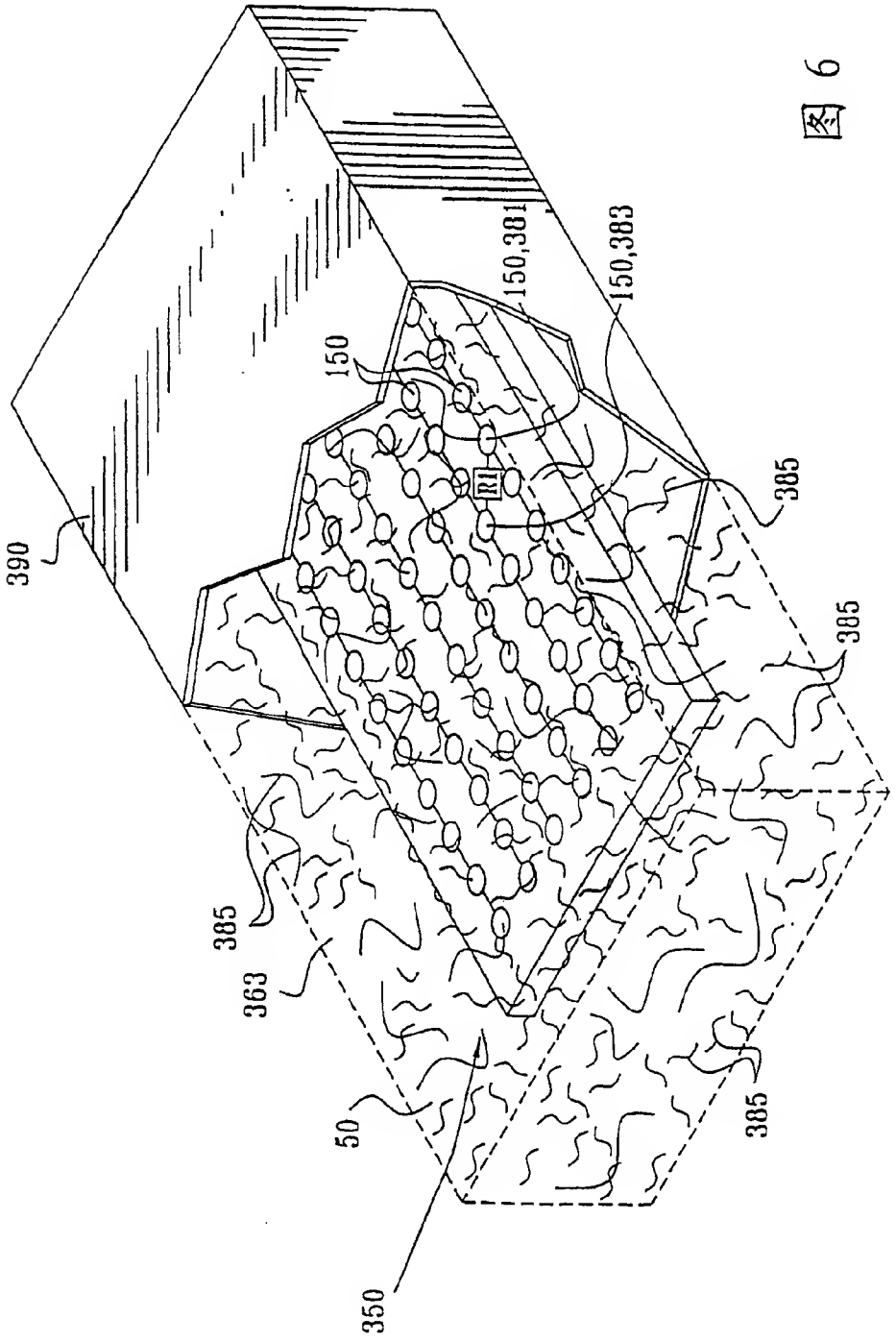


图 6

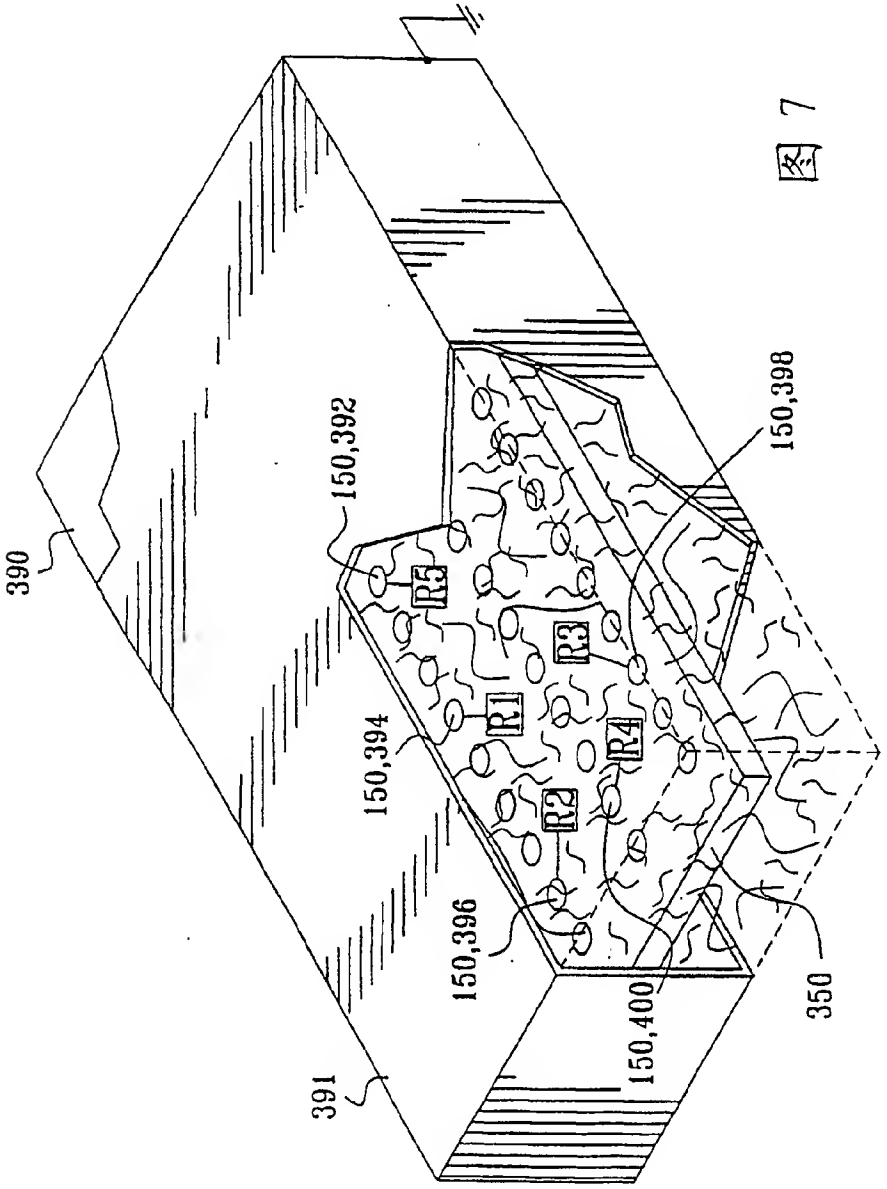


图 7

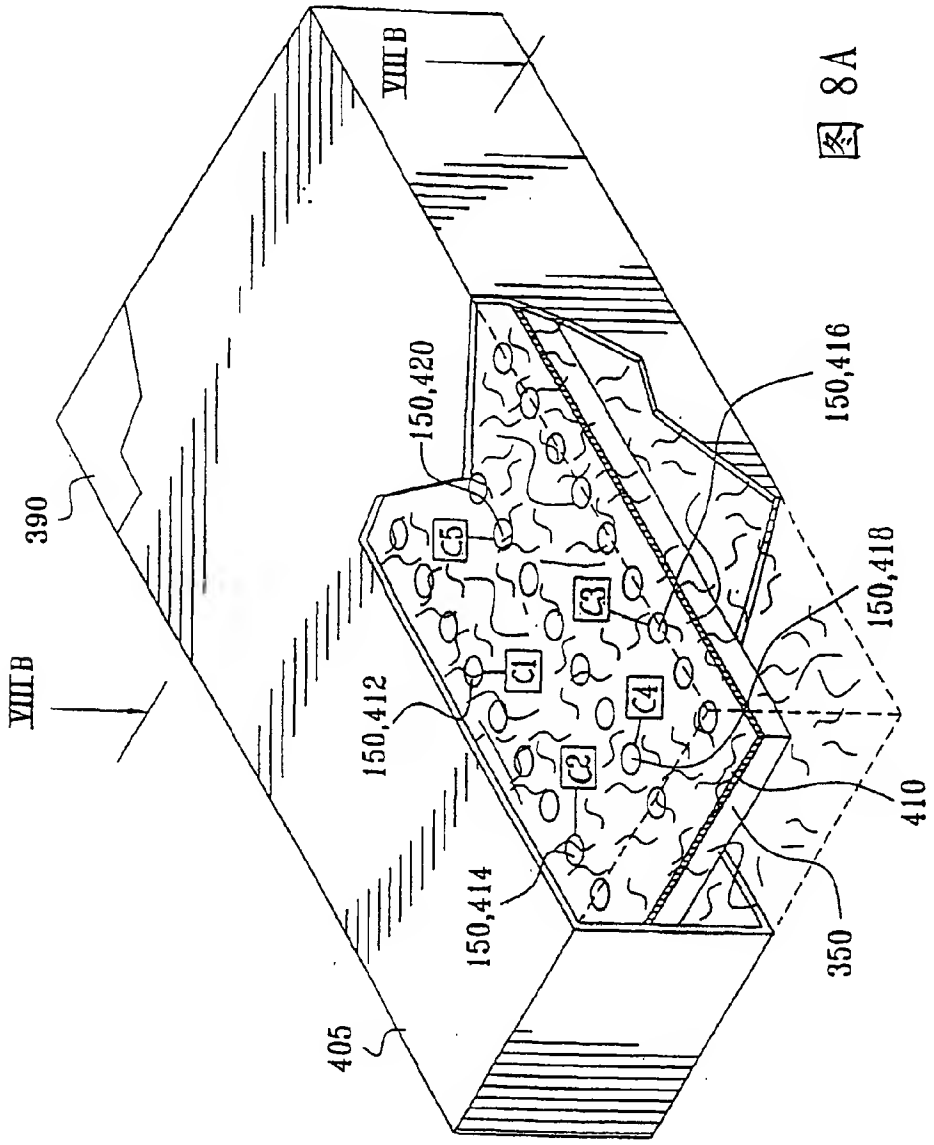

VIII B
VIII B
390
150,420
150,416
150,418
C5
C3
C1
C4
C2
150,412
410
150,414
350
405

图 8A

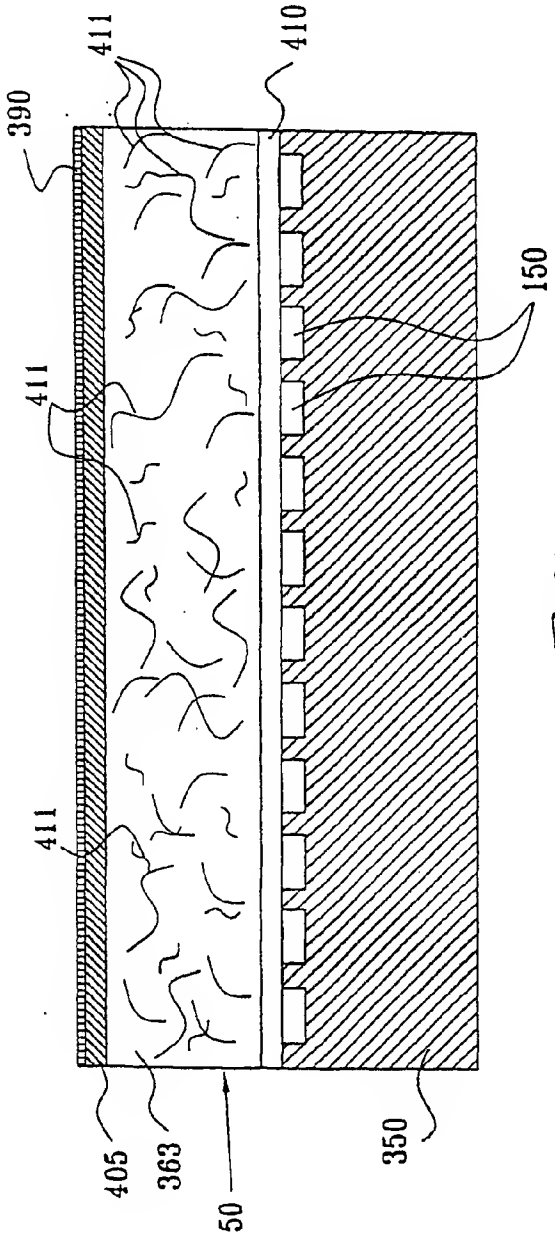


图 8B

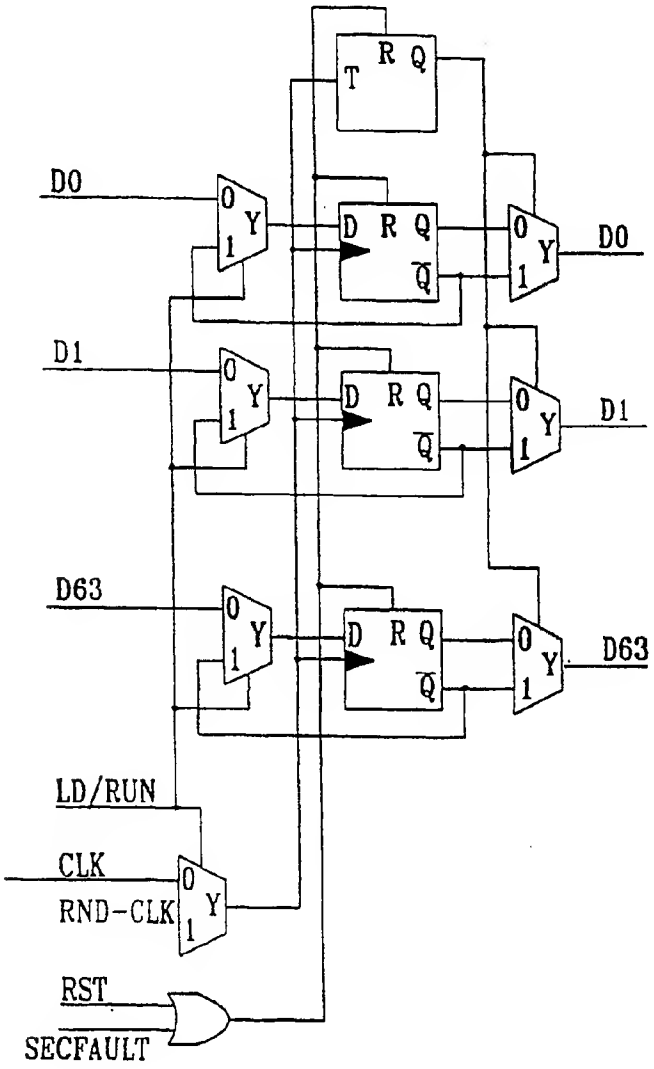


图 9

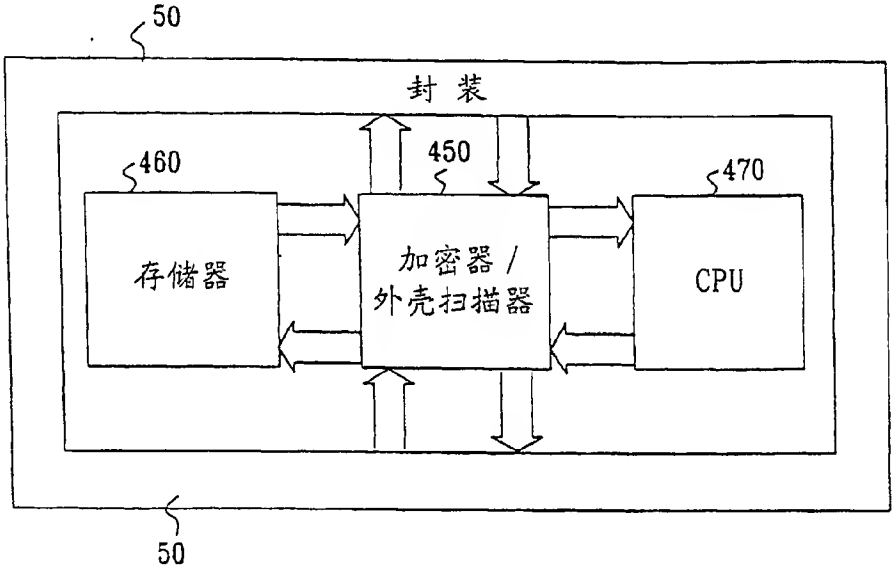

50
封 装
460
450
470
存储器
加密器 / 外壳扫描器
CPU
50

图 10

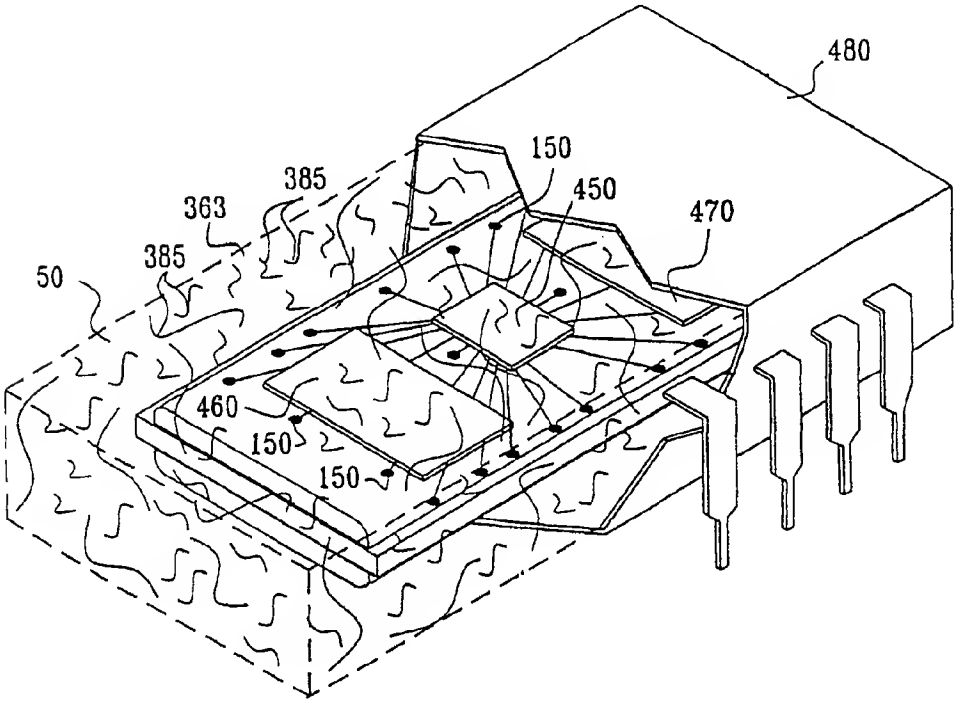

480
150
385
450
363
470
385
50
460
150
150

图 11

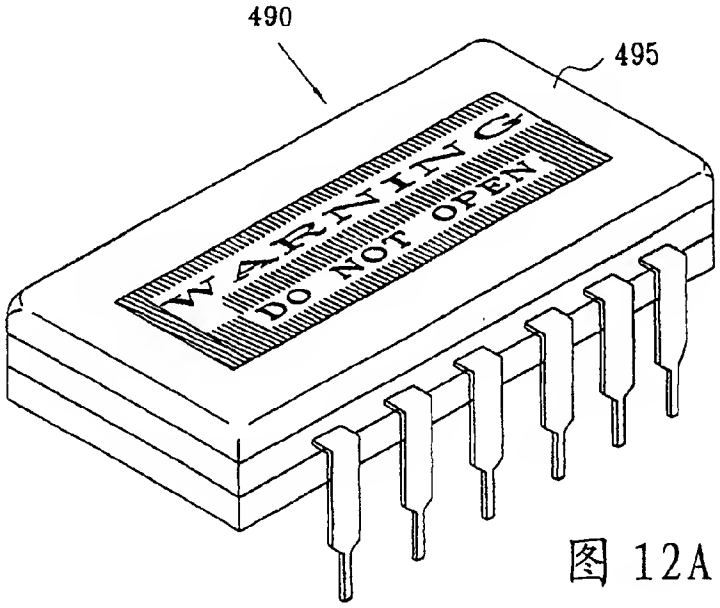


图 12A

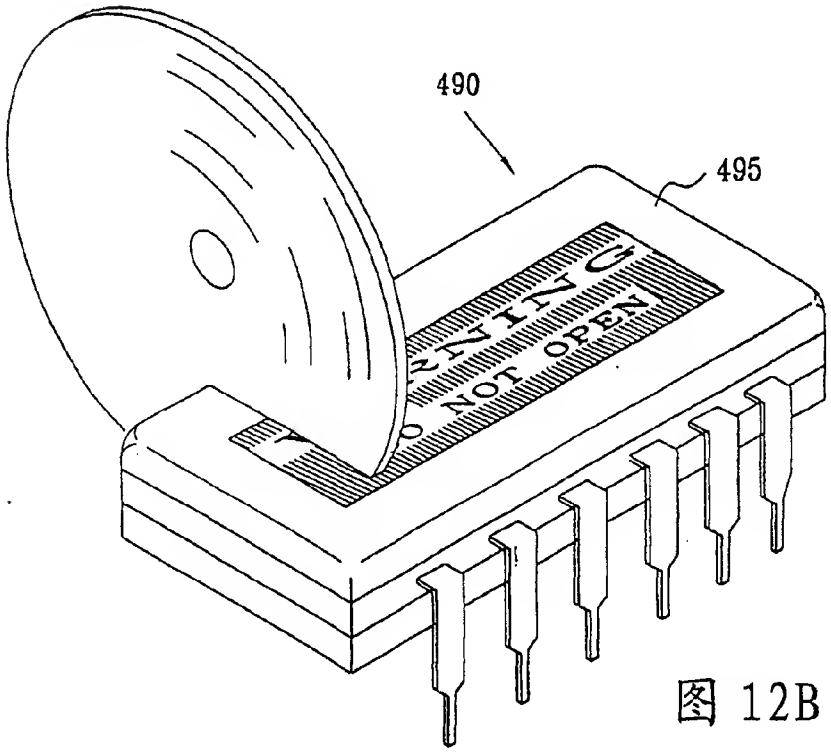


图 12B

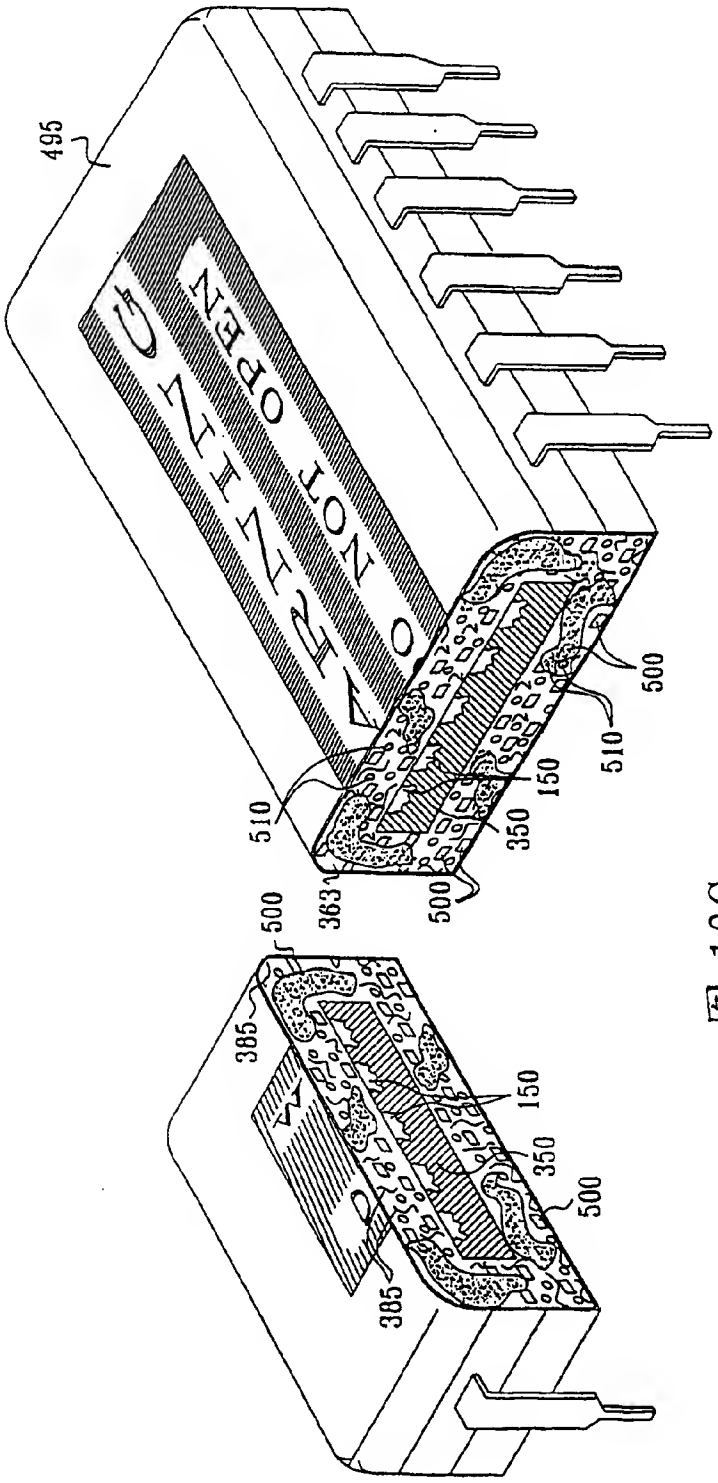


图 12C

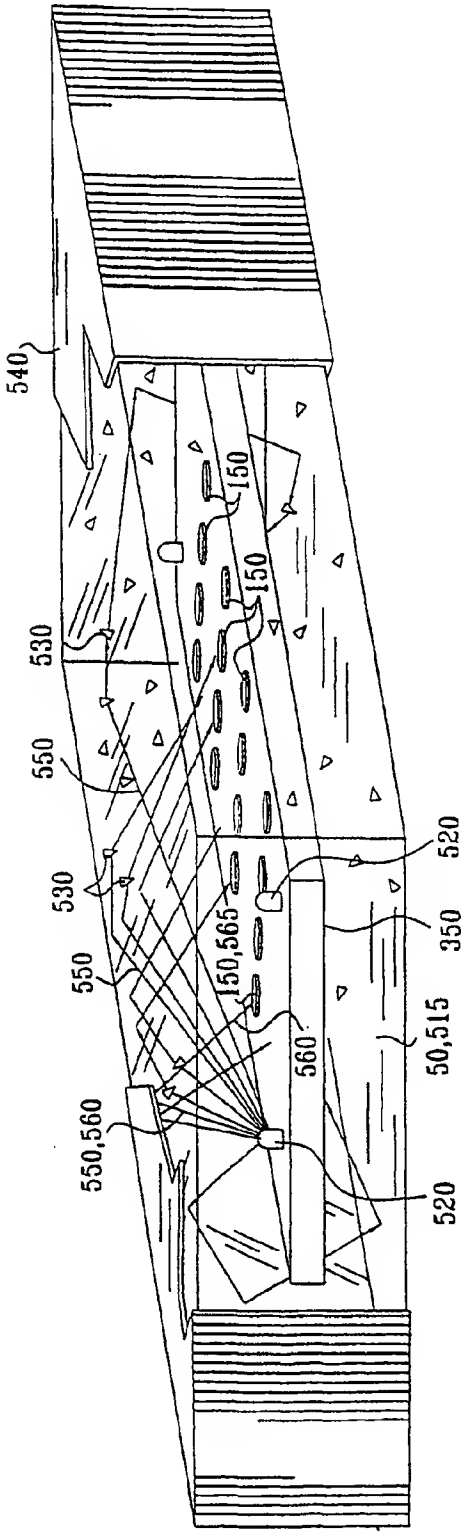

540
150
150
530
550
520
530
350
150,565
550
560
50,515
550,560
520

图 13A

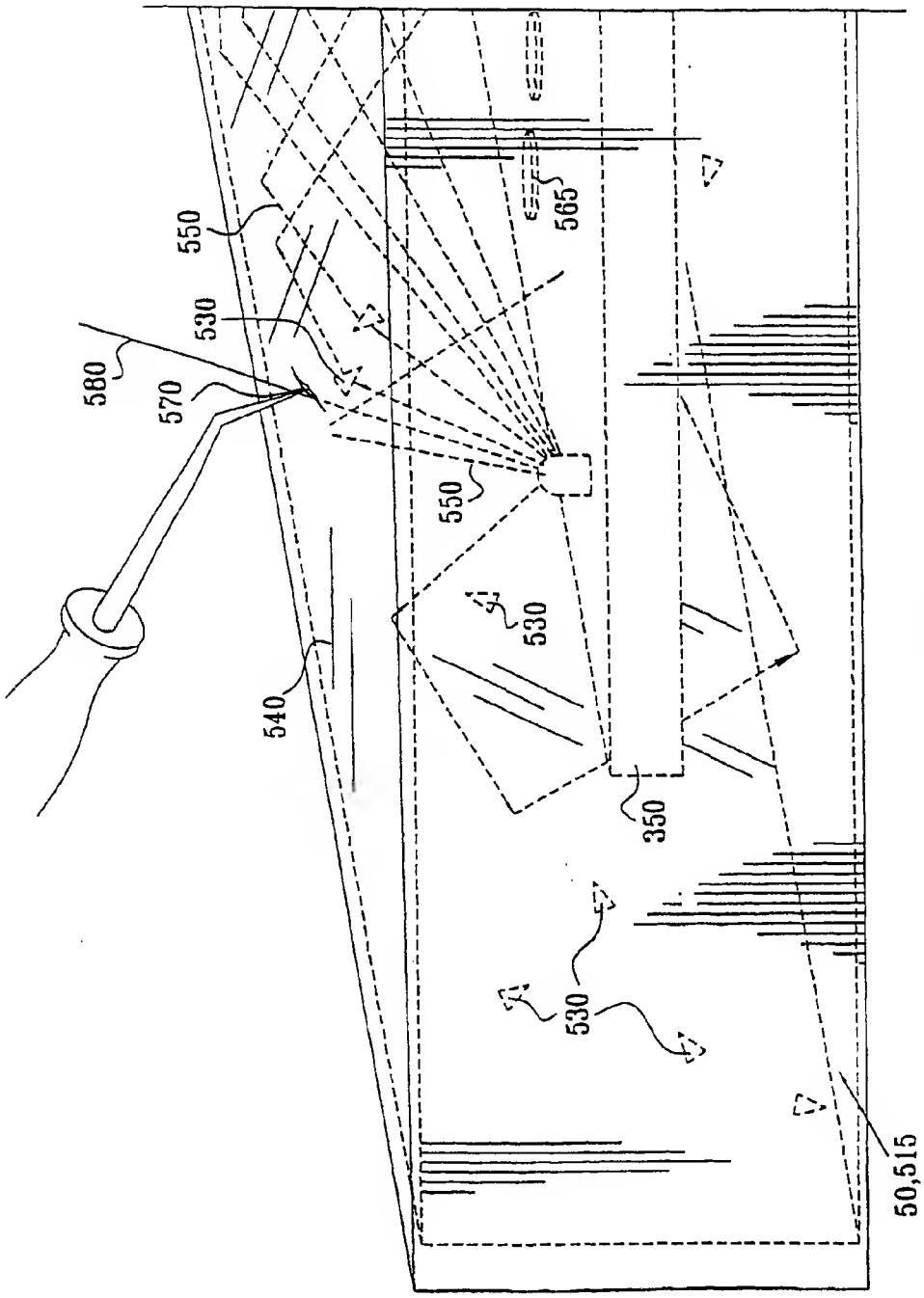


图 13B

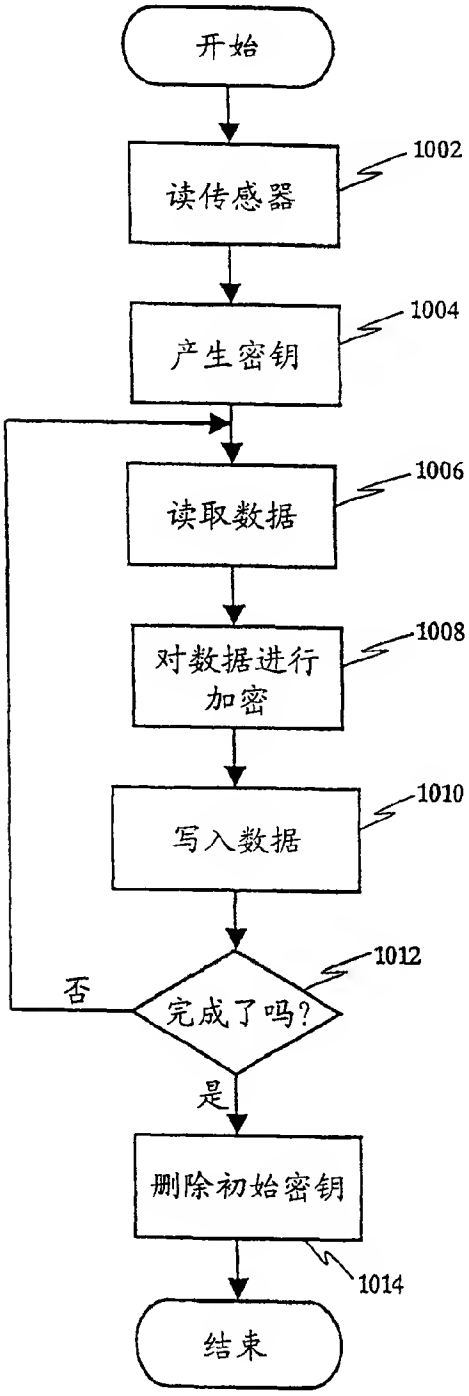

开始
读传感器
1002
产生密钥
1004
读取数据
1006
对数据进行加密
1008
写入数据
1010
完成了吗?
1012
否
是
删除初始密钥
1014
结束

图 14

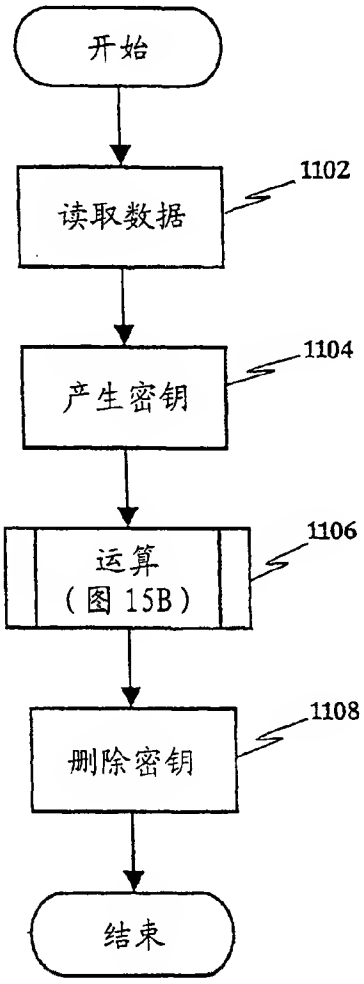


图 15A

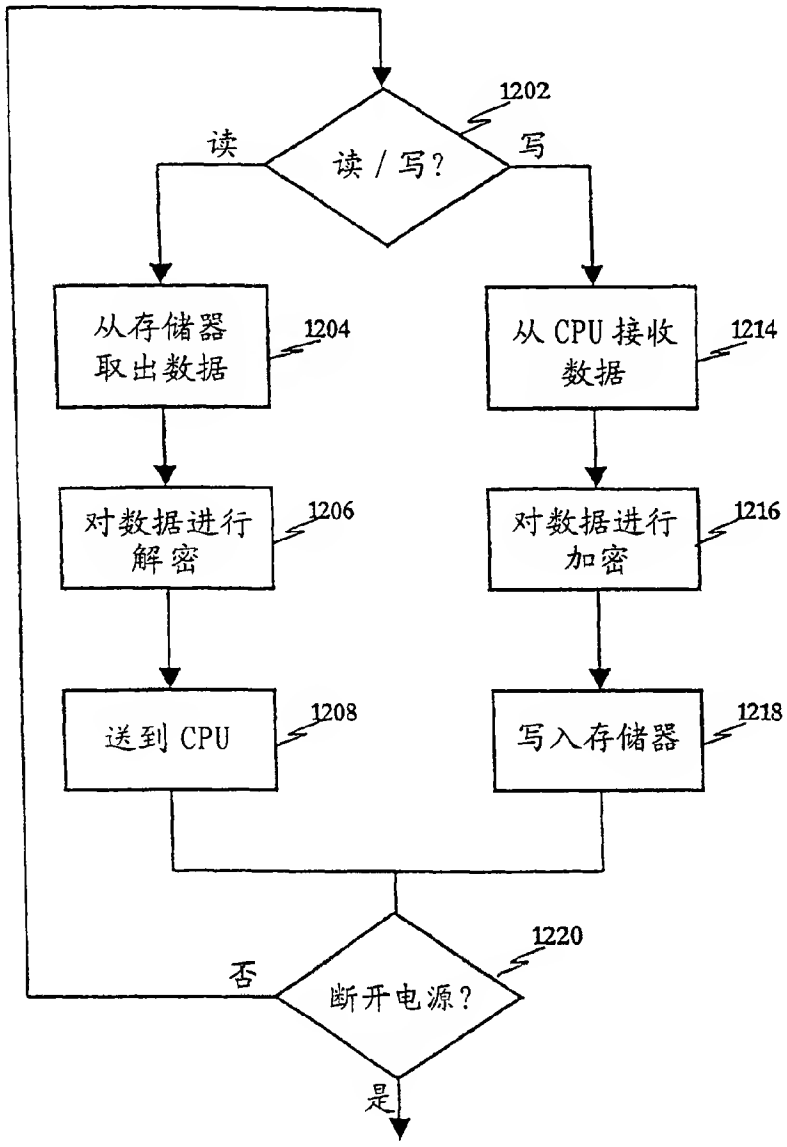

1202
读
读 / 写?
写
从存储器
取出数据
1204
从 CPU 接收
数据
1214
对数据进行
解密
1206
对数据进行
加密
1216
送到 CPU
1208
写入存储器
1218
1220
否
断开电源?
是

图 15B

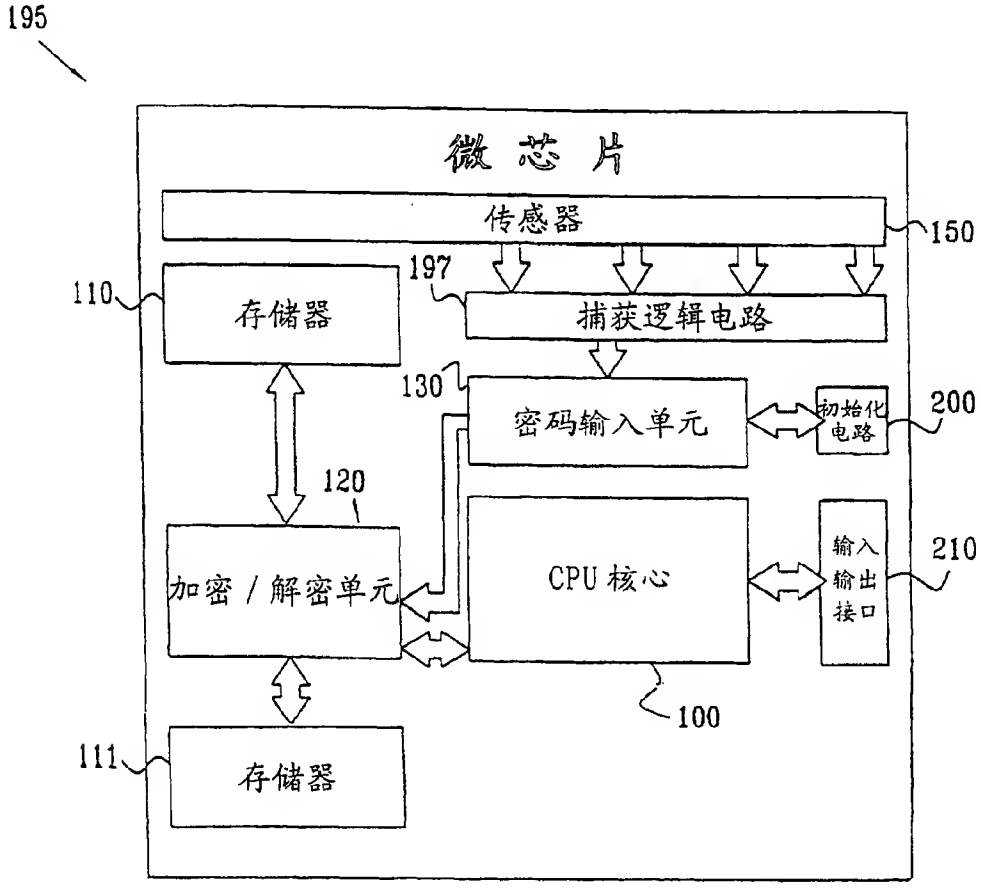

195
微芯片
传感器
150
197
110
存储器
捕获逻辑电路
130
密码输入单元
初始化电路
200
120
加密/解密单元
CPU 核心
输入输出接口
210
100
111
存储器

图 16

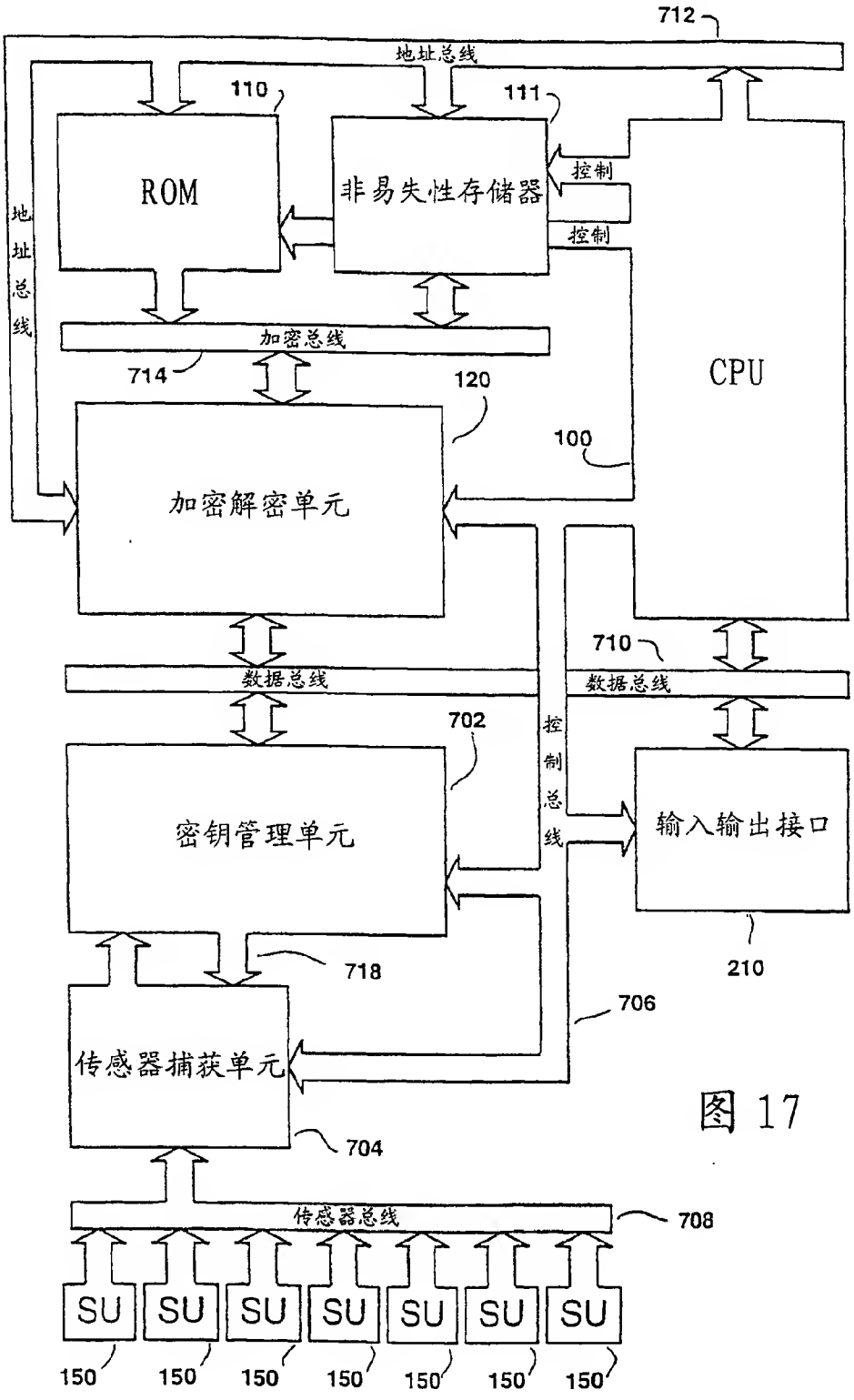

712
地址总线
110
111
ROM
非易失性存储器
控制
控制
地址总线
加密总线
714
120
CPU
100
加密解密单元
710
数据总线
数据总线
702
控制总线
密钥管理单元
输入输出接口
718
210
706
传感器捕获单元
704
传感器总线
708
SU
SU
SU
SU
SU
SU
SU
150
150
150
150
150
150
150

图 17

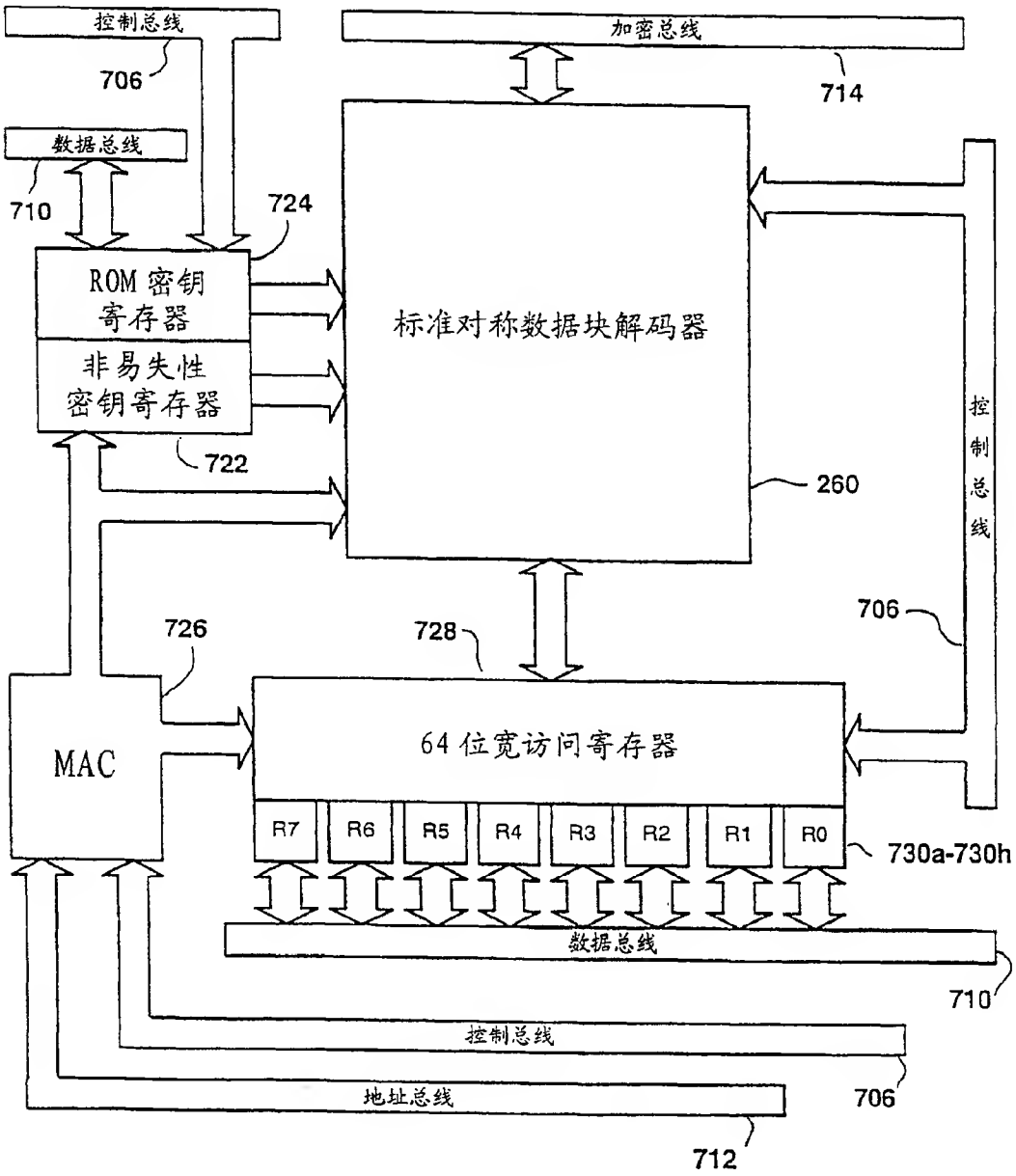

控制总线
706
加密总线
714
数据总线
710
724
ROM 密钥
寄存器
非易失性
密钥寄存器
722
标准对称数据块解码器
260
控制总线
706
726
728
MAC
64 位宽访问寄存器
R7
R6
R5
R4
R3
R2
R1
R0
730a-730h
数据总线
710
控制总线
706
地址总线
712

图 18

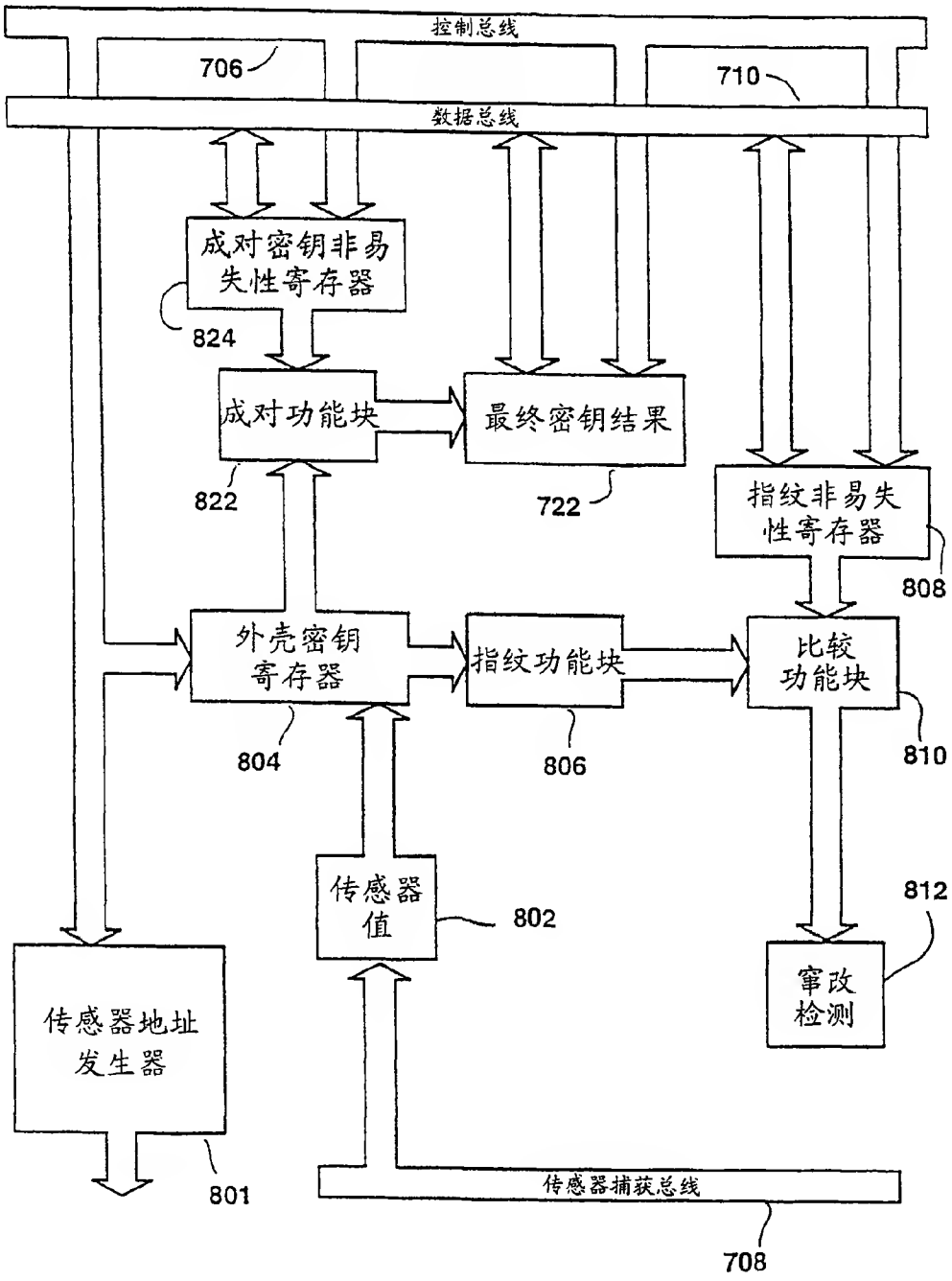

控制总线
706
710
数据总线
成对密钥非易失性寄存器
824
成对功能块
最终密钥结果
822
722
指纹非易失性寄存器
808
外壳密钥寄存器
指纹功能块
比较功能块
804
806
810
传感器值
802
812
审改检测
传感器地址发生器
801
传感器捕获总线
708

图 19

Anti-tamper encapsulation for integrated circuit

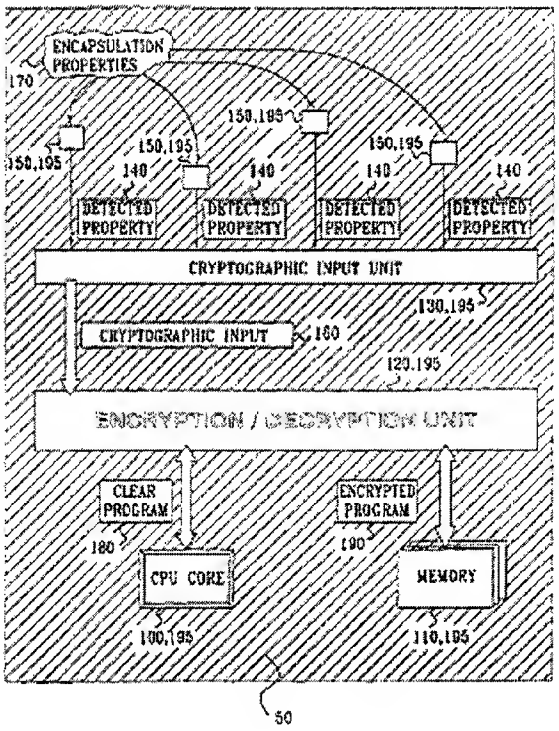
Publication number: CN1433576
Publication date: 2003-07-30
Inventor: KEMERLING OLIVER (DE); KEMERLING FRITZ (DE)
Applicant: KEMERLING OLIVER (DE)
Classification:
- international: ***G06F12/14; G06F21/06; G06F21/24; G06K19/073; H01L21/822; H01L23/58; H01L27/04; H04L9/08; H04L9/10;*** **G06F12/14; G06F21/00; G06K19/073; H01L21/70; H01L23/58; H01L27/04; H04L9/08; H04L9/10**; (IPC1-7): H01L23/58
- European: G06K19/073; G06K19/073A8; H01L23/58B
Application number: CN20008018715 20001227
Priority number(s): US19990173994P 19991230

Also published as:
WO0150530 (A1)
EP1243027 (A0)
CA2395656 (A1)
AU783858B (B2)

Report a data error here

Abstract not available for CN1433576
Abstract of corresponding document: **WO0150530**

An integrated circuit device comprising: a circuit which uses encryption; and a protective member (e.g. encapsulation packaging layer) which reduces access to the circuit; in which the circuit is responsive to at least one physical parameter of the protective member to apply the encryption and/or decryption (e.g. by reading the key therefrom), so that tampering with the protective member to gain access to the circuit causes the encryption and/or decryption to function differently.



Data supplied from the ***esp@cenet*** database - Worldwide